Security Solutions Today

January / February 2016

RETAIL& HOSPITALITY SECURITY

Cover Focus Point-Of-Sale System Breaches – Threats To The Retail And Hospitality Industries

Special Feature Checkpoint Systems' Innovation Session

Security Feature by Xtralis & Arecont Vision

In Focus Interview with Axis Communications & more!

Scan this code to visit our website

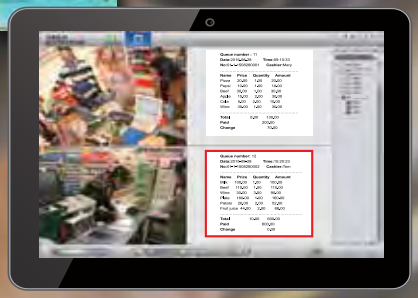
dahua TECHNOLOGY

RETAIL SOLUTION

Better Security, Better Management, Better Business

· Heat Map

· People Counting



· POS Integration

· Mobile Security Management

- Multistage linkages to provide better secured environment
- To create positive shopping experiences for customers
- Provide analysis reports for management strategies-making
- Bring enormous business value to managers

CE FC ISO 9001:2000

DAHUA TECHNOLOGY CO., LTD.
No.1199 Bin'an Road, Binjiang District, Hangzhou, China. 310053
Tel: +86-571-87688883 Fax: +86-571-87688815
Email: overseas@dahuatech.com
www.dahuasecurity.com

www.dahuasecurity.com

secutech ⊗ solution

19 – 21 April 2016 | Taipei, Taiwan
www.secutech.com

SYSTEMS INTEGRATOR FORUM

Sync with

best practices and tech know-hows of IoT, big data, and cloud services in smart city from prominent associations and industry pioneers, including ASIS International, ST Electronics, Siemens, etc.

Source at

Asia's largest security solution show! secutech will take the lead to showcase value-added applications and intelligent surveillance systems, featuring:
- A comprehensive collection from devices, subsystems, to integrated systems and solutions
- Pavilion & themed zones of vertical market

Network with

senior systems integrators onsite to get real-world experiences and hand-on tips.

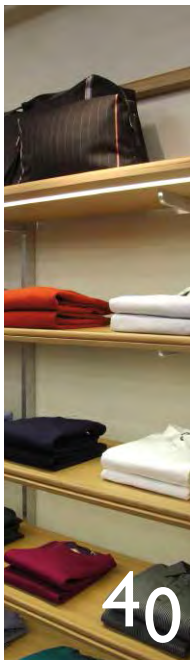
Learn more

Contact us for exclusive int'l visitor package:
Ms. Danielle Lin
danielle.lin@newera.messefrankfurt.com | +886-2-2659-9080 ext. 661

messe frankfurt

CONTENTS

January-February 2016



Big change

is just a small step away.

With Axis surveillance solutions for a safe city you get dependable, crystal-clear HDTV video in real time anywhere you need it. It's easy to coordinate your whole surveillance system centrally – and even share live video.

Plus, you can rest assured that Axis brings a future-proof solution that's ready for today's smart technology as well as tomorrow's.

www.axis.com/safecities

AXIS COMMUNICATIONS

CONTACTS

January-February 2016

Publisher
Steven Ooi (steven.ooi@tradelinkmedia.com.sg)

Editor
Ain Ebrahim (sst@tradelinkmedia.com.sg)

Group Marketing Manager
Eric Ooi (eric.ooi@tradelinkmedia.com.sg)

Marketing Manager
Felix Ooi (felix.ooi@tradelinkmedia.com.sg)

Marketing Executive
Jaslyn Lau (jaslyn.lau@tradelinkmedia.com.sg)

Head Of Graphic Dept/ Advertisement Co-ordinator
Fawzeeah Yamin (fawzeeah@tradelinkmedia.com.sg)

Graphic Designer
Siti Nur Aishah (siti@tradelinkmedia.com.sg)

Circulation
Yvonne Ooi (yvonne.ooi@tradelinkmedia.com.sg)

Photo Credit: William Cho
Designed by Fawzeeah Yamin

Printed in Singapore by KHL Printing Co Pte Ltd.

Security Solutions Today
is published bi-monthly by
Trade Link Media Pte Ltd
(RCB Registration No: 199204277K)
101 Lorong 23, Geylang,
#06-04, Prosper House, Singapore 388399.
Tel: 65-68422580 Fax: 65-68422581
ISSN 2345-7104 (Print)

ANNUAL SUBSCRIPTION:

Surface Mail:
Singapore - S$45 (Reg No: M2-0108708-2 Incl. 7% GST)

Airmail:
Malaysia/Brunei - S$90
Asia - S$140
Japan, Australia, New Zealand - S$170
America/Europe - S$170
Middle East - S$170

ADVERTISING SALES OFFICES

Head Office: Trade Link Media Pte Ltd.
(RCB Reg. No: 199204277K)
101 Lorong 23, Geylang, #06-04, Prosper House, Singapore 388399.
Tel: +65 6842 2580; Fax: +65 6842 1523, 6846 8843, 6842 2581.
Email (Mktg): info@tradelinkmedia.com.sg

India:
Mr. Avneet Singh
Mark Excellence Business Management
C317 / 8 Inlaks Nagar, C.H.S.
15 Yari Road
Versova, Andheri (West)
Mumbai
India
Tel: +91-22 325 81 747
Fax: +91-22 263 96 204
avneet@markexcellence.com

Korea:
MCI
Rm. 103-1011,
Brown Stone, 1330,
Baeseok-dong, Goyang-si,
Gyunggi-do,
Korea 410-907
Tel: +82 2 730 1234
Fax: +82 2 732 8899

Japan:
T Asoshina/Shizuka Kondo
Echo Japan Corporation
Grande Maison, Rm 303,
2-2, Kudan-Kita,1-chome,
Chiyoda-ku, Tokyo 102,
Japan
Tel: +81-3-32635065
Fax: +81-3-32342064

Italy/Switzerland:
Arch. Aldo Cacchioli
Publistein di
Galli-Cacchioli & Co.,
Via Borghese 11
CH-6600 Locarno
Switzerland
Tel: +41-91-7516910
Fax: +41-91-7517109
info@publistein.com

Merchandise Availability Solutions

The Intelligent Loss Prevention Solution for Retail

Combining the flexibility of the E10 2.0 RF/RFID antennas with the real-time benefits of S3i technology

- RF and/or RFID Technology
- Integrated visitor counting
- Improves customer experience
- Real-time notifications and alerts

Let us help you create an exceptional shopping experience, increase security and reduce out-of-stocks.

Email: Apac.Marketing@checkpt.com
Find out more at:
CheckpointSystems.com

Checkpoint®

Intersec Dubai 2016

Date: 17th to 19th January 2016
Venue: Dubai International Convention and Exhibition Centre
Organiser: Messe Frankfurt Middle East GmbH
Contact: Andreas Rex
Tel: +971 4389 4500
Email: andreas.rex@uaemessefrankfurt.com
Website: www.intersecexpo.com

ISC West 2016

Date: 6th to 8th April 2016
Venue: Sands Expo Centre, Las Vegas
Organiser: Reed Exhibitions
Contact: Kelly Miller
Tel: (203) 840 5559
Email: kmiller@reedexpo.com
Website: www.iscwest.com

Secutech Taiwan 2016

Date: 19th to 21st April 2016
Venue: Taipei Nangang Exhibition Centre
Organiser: Messe Frankfurt New Era Business Media Ltd
Contact: Echo Lin
Tel: +886 2 2659 9080 ext. 660
Email: stvn@newera.messefrankfurt.com
Website: www.secutech.com

Cards & Payments Asia 2016

Date: 20th to 21st April 2016
Venue: Suntec Singapore Convention and Exhibition Centre
Organiser: Terrapinn Pte Ltd
Contact: Bess Delarosa
Tel: +65 6322 2734
Email: bess.delarosa@terrapinn.com
Website: http://www.terrapinn.com/exhibition/cards-asia/

Asian Securitex 2016

Date: 4th to 6th May 2016
Venue: Hong Kong Convention & Exhibition Centre
Organiser: Hong Kong Exhibition Services Ltd
Contact: Karina Yu
Tel: +852 2804 1500
Email: exhibit@hkesallworld.com
Website: www.hkesallworld.com

IFSEC International 2016

Date: 21st to 23rd June 2016
Venue: ExCel London One Western Gateway, Royal Victoria Dock
Organiser: UBM EMEA
Contact: Gerry Dunphy
Tel: +44 (0) 207 921 8063
Email: gerry.dunphy@ubm.com
Website: www.excel-london.co.uk

Secutech Vietnam 2016

Date: 18th to 20th August 2016
Venue: Saigon Exhibition & Convention Centre (SECC)
Organiser: Messe Frankfurt New Era Business Media Ltd
Contact: Eva Tsai & Echo Lin
Tel: (886) 2 2659 9080
Email: stvn@newera.messefrankfurt.com
Website: http://www.secutechvietnam.com

MicroEngine®

Integrated Security Systems

The Trusted Brand in Security Solutions

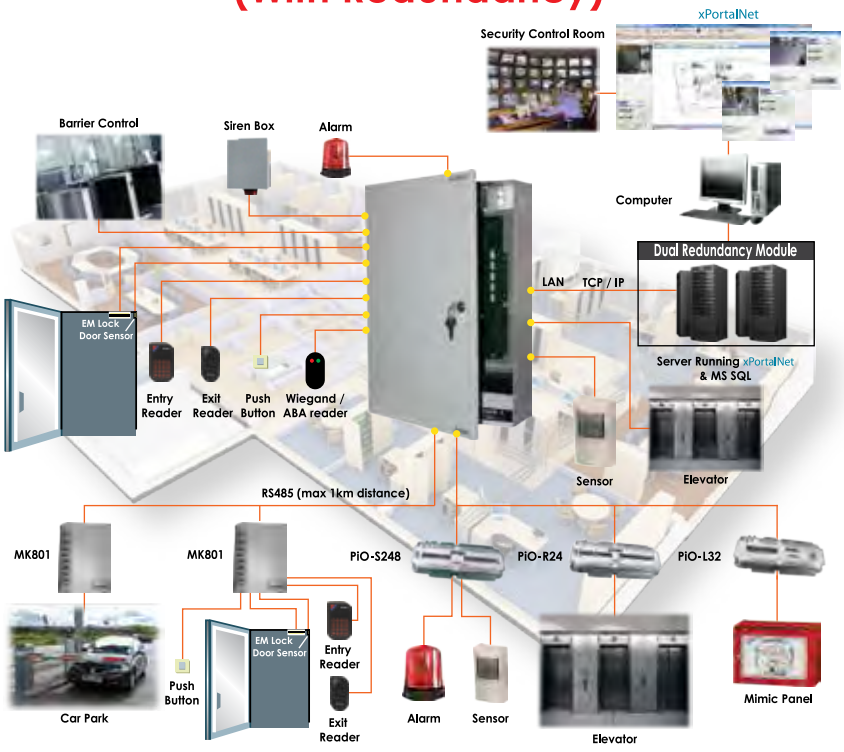
Plato DesFire Reader

- 64 Bit Programmable Card ID
- Encrypted with 3DES
- Card ID Not by Serial Number

P1000i PoE Controller

- PoE with Battery Charger
- AES128 Encrypted IP
- Support 1 Door/2 Readers

Integrated Security System (With Redundancy)



Projects

Commercial / Complex

Factory

Condominium

Plato Reader - Slim Card Reader

600+ readers ward access & security system on SQL Server for hospital and many more ...

enquiry@microengine.net

www.microengine.net

Our Office

Editor's Note

Hello dearest readers of Security Solutions Today!

Let's start with SST wishing all of you a happy brand-new 2016 – keeping those resolutions intact, I hope! Looking forth, SST enthusiastically welcomes the New Year whilst presenting to you, our latest, engaging and thought-provoking JAN/FEB issue filled with enticing retail security articles.

Kicking off this issue, SST knocks down the walls of hacking point of sales. Our 'Cover Focus' comprises of David Siah, Country Manager from Trend Micro as he shares with us the PoS device and network setup weaknesses in retail and hospitality settings that often go unnoticed and unaware. Read on to our 'Inside Look' as Sanjay Rohatgi, Senior Vice-President of Asia Pacific and Japan from Symantec equips retail solution seekers on how to protect PoS systems from attacks.

Join Checkpoint Systems' Innovation Session in our JAN/FEB's 'Special Feature' as they bring you on a tour, showcasing their system and device inventions meant just for retailers. Also in the 'Special Feature' Eddie Ang, General Manager, Asia Pacific, Channel Partners of Checkpoint Systems sits down with us to have a face-to-face interview about the retail industry, its future and the road that Checkpoint Systems is headed towards.

Gracing the pages on our 'Security Feature' is Arecont Vision furnishing us on the fundamentals of Wide Dynamic Range and its limitations. In this issue, SST also features Xtralis on their take of how new mobile surveillance cameras can ensure the best and quickest response to emergency cases.

Also for this JAN/FEB issue, SST has had the privileged of having an interview with Martin Gren, co-founder and member of the Board in Axis Communications educating us on the Internet of Things (IoT) and Sanjay Aurora, Managing Director, Asia Pacific of Darktrace giving us a peek at a new perspective in combating cyber threats.

It has been a wondrous journey in preparation of this issue. I hope it will be an informative, enjoyable and educational piece for you.

I wish you all an insightful read!

Cheers,

Ain Ebrahim

BMAM EXPO ASIA 2016
www.maintenance-asia.com

GREEN BUILDING & RETROFITS EXPO ASIA 2016
www.greenbuilding-asia.com

21 22 23 SEPTEMBER 2016

Hall 5, IMPACT Exhibition & Convention Center, Bangkok, Thailand

Why Should You Exhibit?

- **Discover** the world's latest technology that you would never see
- **Update** yourself with latest technology and add it into your business to gain new comparative advantages
- **Establish** new partnerships with exhibitors from leading companies around the world
- **Find** the perfect solutions for your projects and facilities
- **Acquire** valuable knowledge
- **Gain** fascinating information about the industry
- **Expand** your professional circles with over 10,000 trade visitors
- **Get** to know everything you will learn a lifetime in only 3 days

The Power of Exhibitions
Your face-to-face marketing platform
to generate sales leads

www.maintenance-asia.com
www.greenbuilding-asia.com
facebook.com/BMAMExpo
facebook.com/GBRExpo
linkedin.com/in/bmamexpoasia
linkedin.com/in/gbrexpoasia
Youtube: BMAM & GBR Expo Asia

The Asian Construction Week

ASIAN CONSTRUCTION WEEK
BMAM EXPO ASIA 2016
GREEN BUILDING & RETROFITS EXPO ASIA 2016
PULIRE ASIA PACIFIC
CONCRETE ASIA 2016

Organizers

IMPACT Exhibition Management Co., Ltd.
Bangkok Land Building, 10th Floor, 47/569-576, Moo 3, Popular 3 Road, Ban Mai Sub-district, Pakkred District, Nonthaburi 11120
Mr. John Kelvin Esguerra (Overall)
Tel: +66 2833 5358
Fax: +66 2833 5127 to 9
Email: jkesguerra@impact.co.th
Ms. Wong Wing Yan (International)
Tel: +66 2833 5013
Email: wingyanw@impact.co.th

IMPACT MUANG THONG THANI

SPHERE Exhibits Pte. Ltd.
Mr. Aaron Ann – Asst. Project Manager, Trade
Tel: +65 6590 3415
Email: aaronann@sph.com.sg

sphere

Dallmeier Introduces New Videos On The Viewing Software Smavia Viewing Client

Smavia Viewing Client is a powerful and intuitive software for the convenient evaluation of live and recorded image material via Ethernet. In new "How-To" videos, Dallmeier shows how easy it is to use the software and what useful features it offers.

Video "Live View"

This video focuses on live viewing of video material. In the Smavia Viewing Client the cameras are represented in a clear camera tree structure, from which they can easily be moved by Drag & Drop into various split windows. A special highlight are the "flexible split windows": In addition to predefined split views every user can adapt the software specifically to his or her requirements and define and design split windows individually. A corridor mode can also be set up very easily, since there are no fixed default image layouts such as 16:9 or 4:3. If several monitors are being used it is also possible to start the Smavia Viewing Client in multiple instances. In addition, many other useful features are available to the operator, such as the integration of site maps, an easy-to-use zoom function or pixelisation of moving objects.

Video "Search and Backup"

This video deals with the subject of search and backup. Here, Dallmeier introduces the various search functions of the Smavia Viewing Client and explains step-by-step how to efficiently evaluate recorded image material. In addition to a simple search by date and time, other available options include a fast search with user-defined time units and step lengths, an index search for incidents and an extended search for data from external devices such as scanners of cash registers or ATMs. The most efficient evaluation is offered by a search using Dallmeier SmartFinder, a system for intelligent searches for movement within freely definable image areas. Dallmeier uses an example to clearly explain how SmartFinder works. There are also demonstrations of how to create backups of relevant sequences.

For more information, please visit: www.dallmeier.com SST

On The Occasion Of Its 15th Anniversary Evolis Introduces The Primacy Black Edition Of Its Flagship Card Printer

Evolis introduces the Primacy Black Edition, a revamped version of its flagship printer, Primacy. This stunner is being launched to celebrate the 15th anniversary of Evolis. The Primacy has recently been loaded with new features, has outperformed all competition in the plastic card printers market, barely three years after its debut.

A clean-cut and classy design

With a production of only 2, 000 units, this limited edition capitalises on the Primacy Duplex Version, designed for double-sided card printing. The new printer model boasts of a very gracefully crafted body in red and glossy black, along with carbon effects that dress up both sides. These finishing touches are very-out-of-the-ordinary features for a card printer, serving as the trump card for sleekness and elegancy, making this machines a truly high-end printer.

Besides its paying tribute to Evolis' 15th anniversary, this limited edition evidences the flexibility and responsiveness of Evolis' advanced facilities and resources for production. From design, to development and production this printer was up and running within a very short timeframe.

The Primacy Black edition is shipped with cardPresso XS Edition, a user-friendly software tool to design and personalise plastic cards, with the help on a database if required. In addition, a colour ribbon with a capacity of 200 printings is included, along with 100 blank cards.

Top-notch performances

Primacy makes all the difference, thanks to its ease of use, flexibility and ultra-fast operations. Loaded with advanced technologies, this printer supports all card printing and encoding requirements for medium to large runs. With the recent addition of new features, the printer benefits from increased performances, flexibility and security. Novelties include extended memory size and printing resolution, a low-card level sensor, an update verification wizard, and an UHF encoder. Other features are scheduled to be implemented by the beginning of next year, and include an LCD screen, increased printing output for monochrome printing, an electronic locking system.

"With more than 50, 000 printers sold and over 500 million cards printed since its launch in 2012, Primacy has rapidly turned into a market benchmark when it comes to printing quality and flexibility. The Primacy Black Edition capitalises on Evolis' flagship printer, and highlights once again the reason why Evolis has remained unbeaten over the past 15 years: "innovation", says Delphine Bidaud, Product Manager for Primacy Evolis.

For more information, please visit: www.evolis.com SST

GJD Expands Its D-TECT IP Range

GJD has expanded its D-TECT IP range with the launch of the new D-TECT 3 IP external motion detector, which utilises quad element PIR and microwave technologies and smoothly integrates with third party VMS providers and CCTV systems.

The D-TECT 3 IP works in conjunction with a bespoke and user-friendly web based interface, affording intuitive and quick online access. The user can change all of the detector settings remotely via the interface. Some of the adjustable settings include the ability to alter the LUX level trigger, sensitivity and detection range, as well as setting activation for specific times. A major benefit is that no software or installation is needed for the interface as the user simply logs in via a web address. Working in conjunction with CCTV systems, the D-TECT 3 IP can instantly direct cameras to the location of intrusion; whilst security personnel are alerted with detailed alarm information by SMS, telephone or email. Owing to the pairing of quad element PIR and microwave detection technologies, the new IP detector provides exceptional resistance to false alarms, making it well-suited to monitor large detection areas for a range of sectors including residential, commercial, industrial, heritage and many more.

Mark Tibbenham, GJD's Managing Director commented: "For customers that require IP based detection, the D-TECT 3 IP combines all of the versatile benefits of the D-TECT 3, which has recently been rated best in its category in Benchmark's independent product group test, combined with IP connectivity, providing highly reliable IP based security detection."

The D-TECT 3 IP offers adjustable viewing settings including, 180 degrees pan and 90 degrees tilt

with visual pan and tilt alignment markers. It also offers a10 degrees to 70 degrees detection angle and a programmable beam range up to 30 metres, avoiding boundary overspill and providing accurate detection, making it particularly effective for perimeter surveillance.

Other key features include the ability to withstand harsh weather conditions, low maintenance and robust IP65 zinc metal housing.

For more information, please visit:
www.gjd.co.uk SST

TÜV Certifies IT Security Of Access Control System Siport

Siemens has had the IT security of its Siport 3.0 access control and time recording system certified by the German certification authority TÜV Trust IT GmbH. All the system's relevant software and hardware components passed TÜV's tests for IT security as well as information and data protection. Siemens is one of the very first companies to demonstrate the high security standard of its access control and time recording system by way of independent certification.

Certified security

The modular Siport 3.0 system for access control and time recording provides users with a high level of data and information security. From the ID and reader to the controllers, servers, clients and web clients, everything is suitable for use in applications requiring an increased level of protection. In addition to this, all communication channels are encrypted. This ensures that only users who have the appropriate permissions can access data. TÜV Trust IT tested all relevant components with regard to IT security in accordance with its extensive catalog of requirements. The development process and environment were also inspected. Siport 3.0 was certified as "TÜV Trusted Application" end of September."

In developing Siport, we focused on making sure the system – from the ID cards to the server – is suitable for implementation in environments with high or extremely high security requirements. This is particularly true for pharmaceuticals companies, airports, and data centres", said Philippe Huysman, Global Portfolio Manager Access Control for the Siemens Building Technologies Division, upon receiving the certificate in Cologne. "With the TÜV certificate, we now also have official confirmation from an independent certification authority that we can offer our customers an access control solution for the highest security demands with Siport 3.0."

For more information, please visit:
www.siemens.com/siport SST

Milestone Makes Access Control Visual For Finnish Company

The Milestone Systems XProtect Access Control Module is being used by Turvatiimi Oyj to ensure a fully integrated visual access control security system to protect the company's new premises.

The Finnish security company had various requirements that their new security system needed to fulfil: handling visitors securely and efficiently, restricting tailgating, avoiding access card misuse and 'spoofing' of access which is when someone gain unauthorised access by falsifying their identity. Since these needs are all inherent risks in traditional access control systems, Turvatiimi Oyj's premises, while providing excellent service to visitors.

The Milestone XProtect Access Control Module has made it possible to integrate Axis access control units with Milestone Systems' leading-edge video management software XProtect Professional for an efficient and future-proof visual access control system. The access control system has been installed to ensure a secure working environment without compromising the convenient interaction between employees working in different parts of the building and the company's visitors.

Turvatiimi Oyj's headquarters in Vantaa has multiple offices equipped with access control. In total, 19 doors are continuously monitored via the Milestone XProtect Smart Client video interface. Thanks to Milestone XProtect Access Control Module, Turvatiimi Oyj has an integrated visual solution that maintains a high level of security for the company's 50 employees and many daily visitors.

"Security managers from other companies often ask me how we can keep track of so many people at our offices, and I just show them how easy it actually is with this combined technology," says Mika Bragge, Head of Technology at Turvatiimi Oyj.

There are 18 Axis cameras and 19 AXIS A1001 Access Control units installed at Turvatiimi Oyj headquarters. All are managed by Milestone XProtect Professional video management software with full integration to the AXIS A1001 door controllers using the XProtect Access Control Module. All employees now have access tokens that can be used at all locations. The system integrates fully with the Responda 113 alarm system, ensuring rapid and informed response if unauthorised access is detected by the system.

"We will use the integrated access control system at all our locations. This will give us the same access control tokens at all our sites, with centralised control at the same time," says Mika Bragge. "So far, the experience with the integrated video and access control solution is very positive. The system is fast for reacting and gives immediate information on incidents."

For more information, please visit:
www.milestonesys.com SST

Hikvision Honors Women In Security

Hikvision USA honoured women in the security industry at yesterday's Karen Marquez Honors, presented by ASIS International's Women in Security (WIS) council. The annual event, now in its third year, recognizes four female ASIS members whose contributions have furthered the growth of women in the security industry.

WIS provides support and assistance to women in the security industry and works to inspire those interested in entering the industry. WIS supports and promotes its global members by utilising collaborated skills and talents to strengthen leadership abilities.

"We stand on three pillars: support, inspire, and promote,"

continue on page 14

explained Gail Essen, CPP, PSP, chair of the WIS Council. "Our strategic plan and the work by our twelve committees encompass these pillars to increase the number of women in the security industry. The Karen Marquez Honors are one way we support and celebrate the efforts of such women."

Karen Marquez was the co-owner and executive vice president of MVM, Inc., a physical security services firm, and had a 23-year career in security. Her service as a member of Women Business Owners and the National Association of Female Executives allowed her to bring her hands-on expertise to global management issues. Ms. Marquez died in 2006 after a long battle with cancer. Her work is carried on today by the Marquez Foundation, an organisation that helps Hispanic students achieve college education together with WIS.

Hikvision was a proud sponsor of the Karen Marquez Honours, and several women from Hikvision attended the event. This year's honourees were Sandie Davies, executive director of IFPO International, Victoria Ekhomu, managing director of Trans-World Security Systems, Julieta Munoz Cornejo, regional vice president for ASIS Mexico, and Susan Walker, regional security manager at the Department of Homeland Security.

Jeffrey He, president of Hikvision USA and Hikvision Canada, remarked on the company's commitment to women in the security industry. "As Hikvision rapidly expands in North America, we continually seek to meet the needs of our diverse array of customers. By building a team that includes a diverse group of men and women, we strengthen our own capabilities with a broader set of backgrounds, and in turn ensure the future of the company's success. Hikvision is pleased to support Women in Security and we offer our congratulations to the Karen Marquez Honourees."

For more information, please visit:
www.hikvision.com SST

Pelco By Schneider Electric's Optera Cameras Capture People's Choice Award At ASIS 2015

Pelco by Schneider Electric announced that its Optera 180, 270 and 360 degree panoramic cameras the 2015 ASIS Accolades Security's Best People's Choice Award Winner. Offering the industry's only multi-sensor camera that produces seamless panoramic video, Pelco's state-of-the-art Optera cameras allow users to immerse themselves within any scene, free of the gaps you find with traditional panoramic cameras. The award was presented during a networking luncheon held at the 61st Annual ASIS International Seminar and Exibits in Anaheim, Calif.

"We are honoured to be recognised by our customers through this prestigious award. After all, it is about the unique user experience with our Optera cameras and users are our customers," said Herve Fages, Senior Vice President, Video Line of Business at Pelco by Schneider Electric. "No other competitor in the market today has an innovative camera solution that produces the seamless, high quality panoramic images that Optera delivers. And, the difference is immediately apparent to users. They no longer have to look past the visual imperfections; with Optera, users only see the cohesive panoramic views, much like the human eye."

Optera was one of 42 new product and service solutions submitted to the ASIS 2015 Accolades Competition. Each year, the awards are voted on by a panel of end users and experts, and are presented to the companies with the most innovative new technology solutions based on level of innovation, unique attributes and the benefit the solution brings to the security industry.

"We could not be more thrilled to be the recipients of such a distinguished award acknowledging the innovation of our Optera cameras," said Kim Loy, Vice President of Marketing at Pelco by Schneider Electric. "And we are so pleased that it was the People's Choice Award because it comes from our customers."

For more information, please visit:
www.pelco.com SST

Morse Watchmans Debuts In Ukraine With High Profile Installation

The new headquarters of 1+1 Media Group has recently opened in Kiev. Before the move, various departments were spread across the city, causing inefficiencies in both workflow and organisational structure. Now, all activities relating to the company's broadcast, social media and content production groups are conducted at the new headquarters, making it easier for staff, temporary employees and visitors to go about business.

Bringing together more than 1,000 employees in an eight-storey building necessitated rigorous planning with regard to logistics and physical security. Access to the building had to be controlled, with different levels of access assigned to various employees. For economic and security reasons, management concluded that door locks with keys would be the best solution for managing access. However, manual management of the keys quickly became a problem; keys were often misplaced, lost or taken without authorisation.

According to Volodymir Tarasyk, Chief Security Officer for 1+1 Media Group, numerous procedures for controlling the keys were tried without success. He says, "There were simply too many people who needed access to keys for a manual system to be effective. We needed somehow to minimise the human factor."

They found a solution with the Morse Watchmans KeyWatcher Touch key control and management system. With the automated system, all keys are secured in a tamper-proof cabinet when not in use and, when needed, can only be accessed by authorised personnel using their access control proximity ID badge to open the cabinet and remove or return a key. Users can only take a key they have been pre-authorised to access and all other keys remain securely locked in the cabinet.

All activity is automatically recorded so Tarasky's department has an accurate record of who accessed keys and when. The systems automatic email notification sends an alert when a key has not been returned remote functions and reports while the server performs all synchronisations of transactions as well as maintaining the SQL database.

"The Morse Watchmans KeyWatcher Touch system is integrated with our existing access control system and this has greatly enhanced the level of security in our building," says Tarasyk. "Manual control procedures have been eliminated and we know who has used or is using each and every key."

In addition to the economic savings realised by using mechanical locks and keys on doors throughout the building, 1+1 Media Group was also able to realise a savings in security personnel. Tarasyk states that by using the automated KeyWatcher Touch system they were able to reduce the number of security posts by two, further enhancing ROI.

The system installed at 1+1 Media Group consists of two 9-module cabinets, each holding up to 144 keys and configured with proximity card readers. Operating language is in Ukrainian.

For more information, please visit: www.morsewatchmans.com SST

Schneider Electric Addresses Burgeoning IOT Growth With Micro Data Centre Solutions For Edge Computing

Schneider Electric announced the introduction of its micro data centre solution portfolio for the UK and Ireland. The range enables data processing to be brought nearer to the point of M2M data production in IOT and other highly automated applications.

Delivered in a single enclosure, the benefits of the new micro data centre solutions include power, cooling and management software to support a self contained, secure computing environment. The factory-built solutions are ideal for customers who need to reduce latency and quickly add capacity while ensuring a secure and easy to manage environment. The solutions offer the option to be supplied as chassis prepared for population, or as ready-to-deploy appliances including IT equipment via systems integration partners.

"Through the micro data centre offer, Schneider Electric is addressing the latency, bandwidth and processing speed challenges customers are facing with the growth of connected devices and data applications," said Kevin Brown, Vice President, Global Data Center Strategy and Technology Schneider Electric. "We are already seeing the emergence of edge applications in retail and industrial applications, and we believe the need for edge computing will only grow as the Internet of Things expands into commercial applications."

Schneider Electric's micro data centre physical infrastructure solutions include the enclosure, uninterruptible power supply (UPS), power distribution, management software (DCIM), environmental monitoring, cooling and security – all tested, assembled, packaged and then shipped together in a factory environment.

Schneider Electric's micro data centre solutions portfolio includes:

- SmartBunker SX: traditional for IT rooms
- SmartBunker CX: optimised for office environments
- SmartBunker FX: ruggedised for any environment
- SmartShelter: multi-rack, ruggedised for any environment

Key solutions benefits include the following:

- Simplified management
- High levels of security
- Optimised installation and operating cost
- Configured, delivered and installed in the shortest possible time
- Reliability via standardisation and factory testing

Industry analysts agree that a unified approach to micro data centres will allow for more seamless adoption at an organisational scale. "Localised or micro data centres are a fact of life, but by applying a self-contained, scalable and remotely managed solution and process, CIOs can reduce costs, improve agility, and introduce new levels of compliance and service continuity," said David Cappuccio, vice president, distinguished analyst and chief of research for the Infrastructure teams at Gartner.

"Creating micro data centres is something companies have done for years, but often in an ad hoc manner. By partnering with vendors, and creating a consistent and standardised architecture, enterprises can regain control of these critical assets, and increase the ability to rapidly introduce site-specific services, while reducing risks and operational costs, and improving service levels." Gartner, "Apply a Self-Contained Solution to Micro Data Centers", David Cappuccio.

Schneider Electric micro data centre solutions are now available throughout UK and Ireland. Each solution has specific options available and can be customised upon request.

For more information, please visit: http://www.schneider-electric.us/en/solutions/system/s4/data-center-and-network-systems-micro-data-center/ SST

Middle East Presents 'Untapped Growth Potential' For Biometric Security Solutions As Leading Providers Gear Up For Intersec 2016

Dubai, UAE: Rapid economic development and increasing security concerns is turning the Middle East into a market of 'untapped growth potential', said the boss of one of the world's leading providers of biometric security and access control solutions.

Young S. Moon, Executive Vice President of Korean company Suprema, said regional governments and corporations are adopting new identification and authentication technologies to boost defences against potential fraud, cyber-threats, and organised crime.

Biometrics are based on individual behavioural and physiological characteristics that are difficult to replicate, with various system technologies encompassing voice, retina, facial, vein and gait recognition, along with fingerprint matching, and DNA identification.

Middle East governments along with a large number of industry sectors, including banks, aviation, oil & gas and retail, are embracing the new technology, making the region a high-focus area for international biometric systems solution providers.

"We consider the Middle East as a key market with untapped growth potential," said Moon, whose company is among more than 100 international exhibitors specialising in the latest biometric security systems at the upcoming Intersec 2016, the world's leading trade show for security, safety, and fire protection. "The market has vigorous economic growth, high acceptance towards biometric solutions and a demand for high-end technology."

Suprema will launch at Intersec 2016 its BioStation A2. Moon said Suprema would look to build on the success of the last 12 months across the Gulf region, where it installed six biometric system projects in the government, education, and aviation sectors.

"The Middle East is of strategic importance to Suprema," added Moon. "Our products and solutions are developed to address large or small business needs covering a vast array of industry segments. There are a number of factors that contribute to instability, whether fraud, cyber-threats or organised crime. Suprema offers next-level biometric security solutions that directly respond to these threats."

According to a May 2015 report by research firm MarketsandMarkets, the global biometrics systems market is expected to reach US$24.4 billion by 2020, growing at a compound annual growth rate (CAGR) of 17.9 per cent between 2015 and 2020. Analysts from TechNavio forecast that biometrics in Middle East will grow even faster at a CAGR of 19.35 per cent over the period 2014 - 2019.

That will come as good news to AllGoVision, an advanced video analytics solution provider, and another exhibitor that specialises in biometrics at Intersec 2016, which takes place from 17th to 19th January at the Dubai International Convention and Exhibition Centre.

AllGoVision will showcase its 3D Facial Recognition System, which uses facial recognition technology via IP video surveillance to compare facial features with a database of stored facial features to identify potential threats – or a VIP customer.

Ashwin Amarapur, Director of AllGoVision, explained: "In city surveillance, the 3D Facial Recognition System is used to identify Black Listed people or known criminals, but in the case of hospitality or banking the use relates more to 'White Lists' – for example, visitors identified as a VIP guests or high net worth individuals.

"The bank or hotel service staff would be alerted of their arrival in advance and can take necessary care of the valued customer or display an automated welcome note in the electronic board at the entrance," added Amarapur.

Other headline exhibitors at Intersec 2016 with biometric security solutions include the Dubai-headquartered Business Automation & Security System (BASS), Iris ID from the USA, Swiss company Touchless Biometric Systems and WatchNet Access from Canada.

"In the not-to-distant future, everyone in the Middle East could soon replace pin codes with finger prints or Iris scans at an ATM when withdrawing money," said Ahmed Pauwels, CEO of Messe Frankfurt Middle East, the organiser of Intersec.

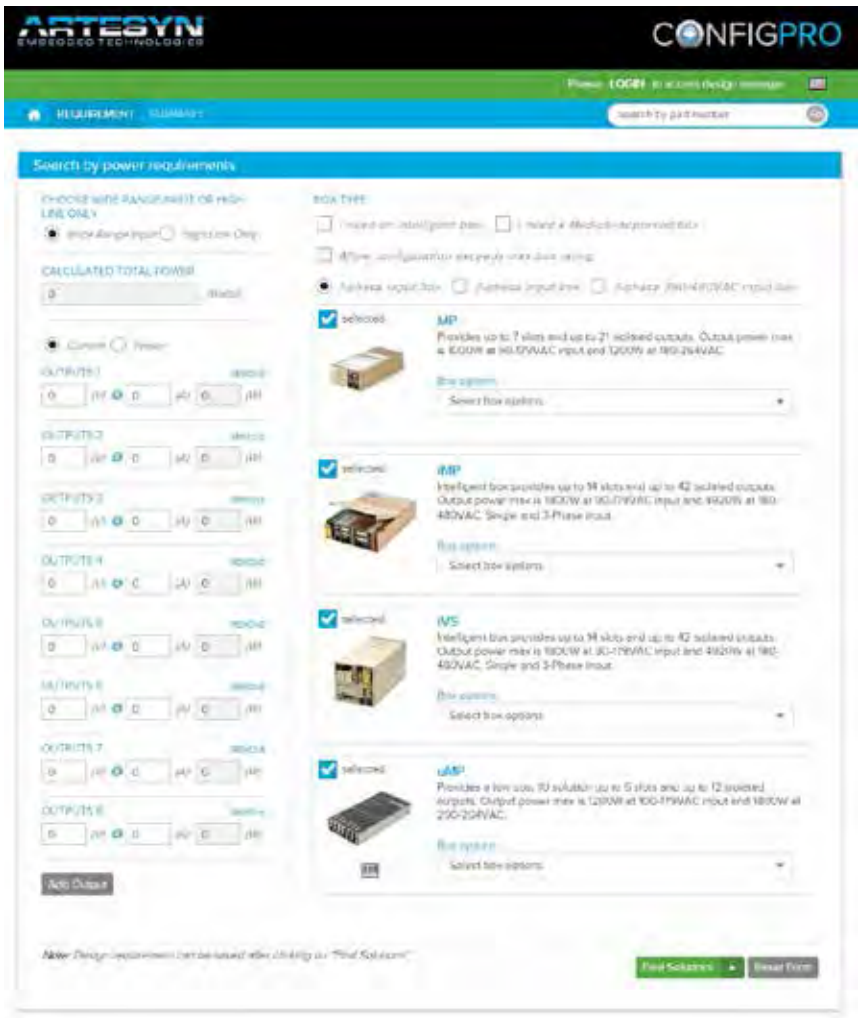
"The possibilities offered by biometric security technologies are vast, whether for government purposes or for the various range of industry verticals, and they'll all share the spotlight when Intersec returns in early 2016."

Now in its 18th edition, Intersec 2016 will feature more than 1,300 exhibitors from 52 countries, spanning over 50,000sqm.

For more information, please visit: www.safetysecurity.messefrankfurt.com SST

New Artesyn Config Pro Tool Simplifies Access To Millions Of Power Supply Combinations

Artesyn Embedded Technologies announced the Config Pro online power supply configurator to help customers find the optimal solution from the three million plus combinations enabled by its range of configurable power supplies. The Config pro tool will make it easier for industrial and medical equipment designers to specify and use configurable power supplies and can, in many cases, eliminate the need for expensive custom solutions.



Covering Artesyn's four configurable power supply families, the MP, iMP, iVS and MicroMP (uMP) series, the Config Pro tool starts with a user entering the current or power requirements for up to 21 individual outputs, up to 500 Vdc output and up to 970 amps. The tool then generates a selection of configured options, which can be further refined and results in a solution that is optimised for cost. It can also recommend further cost-saving alternatives based on similar feature and power ratings. The user is provided with a graphical representation of the configured power supply and downloadable PDF summary of the configuration.

"The Config Pro tool is a game-changer for applications needing medium and high power multi-output power supplies", said Chris Jones, marketing director for Artesyn Embedded Technologies. "With such a wide range of configurable families, we believe we have the most number of power supply combinations in the industry, and this tool will make it as easy to navigate the options as it would be to select a standard, non-configurable unit. The ability to handle voltage inputs that are 'in between' the standard ratings and the numerous other variables considered by Config Pro tool requires a sophisticated system."

Artesyn's Config Pro tool uses a powerful solution algorithm that factors in complex variables including dual and triple output modules, and parallel and series solutions.

The tool also includes a reverse part lookup to enable designers to quickly find information on parts if they have a configured part number.

For more information, please visit: www.artesyn.com SST

Dahua Technology Secures The Safety Of Grand Military Parade

Dahua technology one of the world-leading manufacturer and supplier of video surveillance products headquartered in Hangzhou, China witnessed Chinese Military Parade in Beijing.

Beijing's massive military parade to commemorate the 70th anniversary of the victory of World War II featured hundreds of pieces of new military equipment and about 12,000 troops. China was unveiled in front of the entire world to show not only the overall national strength, but also put the nation's security surveillance system under the highest-standard real field.

On such a significant day, top level of security surveillance, man force as well as cutting-edge technology from public security, traffic control, armed police and fire administrations were required to ensure "zero threat, zero danger" before, during and after the parade. As a professional security products manufacturer, Dahua participated in this splendid live parade as the only security surveillance provider.

Dahua has fulfilled its duty to keep every solid step of the marching troops monitored during the parade. By using Dahua's outstanding security system, people and vehicles presented at the parade were able to guided and controlled. Hundreds of HD security cameras were specially set on West Chang'an Avenue, west reviewing stand, west of Tiananmen Square and other related strongholds. Among them, Dahua HD Bullet Camera and Network Positioning System mainly

adopted on West Chang'an Avenue play a vital role during the whole parade by 360 degree monitoring to capture every detail clearly.

Network Positioning System equipped with starlight series camera is the highlight among the whole security installations. It features up to max 60fps@720P or 30fps@1080P resolution, allowing recording greater scene details even where the intensity of illumination varies considerably. It boasts WDR image enhancement technology, triple video streams, and Intelligent Video Surveillance. Wide Dynamic Range (WDR) features 120dB and offers high performance in extremely bright, dark areas or in backlight.

Meanwhile, it provides enhanced IR illuminators and offer up to 200 metres clear visibility. The PTZ dome provides pan range of 360 degrees endless, and a maximum speed up to 160 degrees per second. it is security quality and versatility that fully ensures the safety of the parade.

The excellent performance of Dahua's security reflects the development of the nation's science and technology. Dahua, with its secure, self-motivated and controllable national innovative ability, will firmly keep on securing for the safety of our homeland.

For more information, please visit: www.dahuasecurity.com SST

Grand Opening Of Bosch Security Systems' Asia Pacific Customer Experience Centre In Singapore

Bosch Security Systems celebrated the launch of its Asia Pacific Regional Experience Centre in Singapore with over 80 key partners and guest from the region. Located in the Robert Bosch headquarter (SEA) building at Bishan, Singapore, the Centre provides an avenue for visitors to explore the best and latest innovative products and solutions to offer.

Guests have gained insights on the products on display through a series of informative talks on product developments and technology trends before experiencing first-hand the power of the technology in an exclusive tour of the Experience Centre. Featuring a host of interactive exhibits, the Experience Centre showcases the extensive portfolio of Bosch's security, safety and communications products available for small to large project applications.

Highlights of the security solutions featured at the Centre include the latest ultra-high resolution FLEXIDOME IP panoramic 7000 MP and DINION IP ultra 8000 MP cameras as well as 4K ultra HD storage solutions. Also on display were communications solutions including the Electro-Voice portable and fixed installed professional loudspeakers, the EVID Compact Sound System, DICENTIS Wireless Conference System, new RTS Keypanels and the highly anticipated PAVIRO sound system, which was launched in August.

Wilfred Steeman, Vice President of Bosch Security Systems Asia Pacific, and Takashi Nobuto, President of TOWA Engineering unveiled the Bosch Security Systems Experience Centre, which has been Bosch's partner for over 47 years. The opening ceremony also welcomed numerous media representatives, partners and Bosch associates from the region. With the opening of the Centre, visitors can look forward to exploring the latest products and experiencing the cutting-edge solutions and various applications Bosch offers. "The versatility of this Experience Centre will allow Bosch to demonstrate the latest products and solutions to various groups of stakeholders from project specifiers and consultants to end users.

The Centre is a highly visible representation of Bosch Security's commitment and investment in the Asia Pacific market", commented Steeman.

For more information, please visit: www.boschsecurity.asia SST

Sony Introduces SRG-360SHE, The Latest High-End SRG Series Remote Camera With Brilliant Features

Sony introduces the SRG-360SHE, the latest addition to its range of high definition remote-operated camera line-up, featuring smooth robotic control and excellent image quality. Targeting at news production, live sport production, music videos and reality television, the SRG-360SHE is also ideal for use in lecture theatres, auditoriums and House of Worship, as well as for corporate, governmental and telemedicine applications.

The SRG-360SHE is equipped with Sony's ExmorTM CMOS image sensor, which is capable of capturing Full HD images in low light conditions. Optimum image clarity is further achieved with Sony's unique View-DR and XDNR (eXcellent Dynamic Noise Reduction) technologies. In addition, the presence of lip synchronisation of video and audio functions also contributes to the elimination of unwanted signal delays. "The SRG-360SHE is ideal for multiplatform broadcasting and production applications with its numerous output interface," said Mr. Riki Nishimura, General Manager of Visual Security Solutions Division, Professional Solutions Company (PSAP) at Sony Electronics Asia Pacific. "Building on the success of SRG-300SE, the SRG-360SHE has triple streaming capabilities that allow recording, monitoring and streaming of high quality images as well as 1080p videos simultaneously together with embedded stereo audio.

Users can seamlessly conduct corporate presentations, webcasts and other events where content can be displayed on a connected monitor, streamed live to the web and instantaneously recorded for editing and archive. This exceptional function expands the possibility of high quality recording while streaming with low bandwidth. In addition, the SRG-360SHE enhances user experience with clarity and intelligibility through the option of attaching stereo microphones and fine-tuned with the on-board audio equaliser and auto level control."

Ease with installation

With PoE+ (Power over Ethernet) capabilities, the SRG-360SHE is able to carry IP video and power over a single connection cable and is easy to install with E-flip functions. This gives ultimate flexibility and is extremely useful for sites that are difficult to access while significantly reduce installation costs.

Further, the camera can be controlled remotely via RM-IP10 using VISCA command protocols over standard IP network or RS-422. The embedded web browser also allows simple control of the camera and image preview from any networked PC. With the large red tally light above the lens, the camera gives presenters clear visual confirmation when it is active

Improved PTZ motion modes

The SRG-360SHE is equipped with a powerful direct drive motor which assures quiet, rapid movement to the target position over a wide pan or tilt angle range. With enhanced PTZ mechanism such as PTZ synchronous simultaneous motion, PTZ trace memory in present and PT slow move, smooth, steady camera movements are possible for polished and professional coverage of any scene. With 30x optical zoom range that is accompanied by 12x digital zoom for frame-filling close-ups, images stay clear and sharp even at high-zoom settings with responsive autofocus. Movement tracing can be stored to memory, which is an attractive feature for on-air applications where users can store and instantly recall up to 256 camera positions from a networked PC and web browser.

For more information, please visit: www.sony.com.sg SST

Trend Micro Q3 Security Roundup Report Showcases Vulnerabilities And Aftermath Of Data Breaches

The interconnectivity of technology has led to a point where many devices are potentially vulnerable, and in the third quarter, the real world impacts of cyber attacks became clear. Trend Micro Incorporated announced its security roundup report, "Hazards Ahead: Current Vulnerabilities Prelude Impending Attacks," which analyses the vulnerabilities and repercussions of attacks seen last quarter. The report unravels the aftermath if security breaches, loopholes found in mobile platforms and exploits posing risks not only to user privacy, but also to physical safety. Additionally, these security gaps serve, as a prelude to potentially massive events that Trend Micro believes will greatly impact 2016.

"The evolution of breaches is beginning to take a turn toward real-world effects on enterprises' bottom lines and people's lives," said Raimund Gene, CTO, Trend Micro. "The emergence of numerous vulnerabilities and other data breaches that occurred in this quarter are bound to release more confidential and potentially destructive information to the public, which could then be sold to the highest bidder on the Deep Web."

Data breaches experienced last quarter, such as Ashley Madison, spurred a chain of attacks, in which dumping stolen confidential information in public domains tarnishes victims' reputations, causing far greater damage than simple business disruptions. Cyber criminals, who leveraged the compromised information to launch extortion attacks and blackmail users caused catastrophe for both Avid Life Media, the site owner, and more than 30 million Ashley Madison users – with reports of victim suicides in response to the impact this attack had on their personal lives.

Additionally, security breaches impacting the healthcare industry were prevalent in the third quarter, including the attack on the UCLA Health System where personal records of approximately 4.5 million patients were compromised. In fact, health and personally identifiable information (PII) was the second-most stolen data type out of all data breach categories. These instances reinforce why the healthcare industry continues to be an appealing target for cybercriminals.

Attackers are continuing to set their sights on mobile device users, taking advantage of gaps in security that exists on the iOS and Android platforms. The discovery of vulnerabilities in Android highlighted the need for a more integrated set of security strategies, while modified versions of app creation tools debunked the notion that the iOS walled garden approach to security can spare the platform from attacks.

"As Trend Micro analysts have observed, cyberspace has become more punitive and attacks are no longer isolated," said Tom Kellermann, Chief Cybersecurity Officer, Trend Micro. "To mitigate future breaches and reduce risk, enterprises must focus on intrusion suppression and address the advent of secondary infections. Integrating breach detention systems with intrusion prevention systems is fundamental to decreasing the time hackers dwell on their networks. Organisations should expect to be hit, and preparing to overcome this challenge will become the mantra in the winter of 2016."

The following are a few report findings, highlighting third quarter activities:

- Data breach dumps were used to fuel further attacks and extortion. The successful attacks against The Hacking Team and Ashley Madison greatly affected the security and computing industries
- Discovery of weak points in mobile platforms emphasise existing problems in both ecosystems. In response to the recent spate of Android vulnerability discoveries, Google finally announced regular security updates for the platform
- Cybercriminals use the "shotgun approach" on PoS malware, primarily affecting small businesses. Attacks seen in the third quarter involved PoS malware launched through "old" techniques like spamming, as well as tools like macro malware, exploit kits and botnets
- Political personalities surface as targets of on-going espionage campaigns. Analysis of recent data revealed that Pawn Storm has expanded its targets from mostly U.S. targets to Russian entities
- Angler Exploit Kit continues to be a widely used tool, with access numbers increasing by 34 per cent. Angler Exploit Kit creators updated their arsenal this past quarter, which resulted in attackers using their creation to distribute new malware
- New research raises issues on the security of Internet-ready devices. Attackers are now modifying target-tank information, which could have dire consequences for the general public.

For more information, please visit: http://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/vulnerabilities-prelude-impending-attacks SST

VIVOTEK Secures India Cosmos Bank's Greatest Asset: The People Of Pune

VIVOTEK is pleased to announce the successful installation of 132 VIVOTEK network cameras across the headquarters of the India Cosmos Bank, the second oldest and largest bank in India. Thanks to cooperation with professional partner, Bajaj Electricals, the Cosmos Bank is now under the protection of VIVOTEK's IP surveillance solutions.

Established in 1906, the Cosmos Cooperative Bank has recently completed an impressive 109 years of service, with multi-state attained in 1997. Cosmos Bank operates a huge network of 140

continue on page 25

branches in India spreading across 7 states and in 39 major cities. The headquarters of bank is in a building with an inbuilt data centre and high security safe in the centre of Pune, a thriving metropolis with a population of five million people. In order to come up with a complete security system to minimise the risk impact, Cosmos Bank engaged Bajaj Electricals to deploy VIVOTEK's solutions to meet three key risks: threats to people, to property and to the image of the Bank.

A total of 132 VIVOTEK network cameras were deployed, including 103 FD8136 ultra-mini fixed dome network cameras for the main floor area, the lifts and the lobby. The FD8136 features a megapixel sensor, while its tiny size of only 90 mm in diameter offers discreet protection for visitors. For the basement parking area, 29 IP8335H bullet-network cameras were utilised.

This camera features day and night functionality and IP67-rated weather-proof housing, allowing Cosmos Bank to build a cost-effective IP surveillance system without additional accessories. Finally, 4 SD8326 speed dome network cameras secured the periphery of Cosmos Bank's headquarters. With a sophisticated pan/tilt mechanism, this camera provides fast, precise movement with continuous 360-degree pan and 220-degree tilt. It also offers audio detection; by recognis9ing increases or decreases in sound volume, an additional layer of intrusion detection is ensured.

Sanjeev Gulati, Country Manager of India & SAARC, VIVOTEK said, "There are many exterior factors that have to be considered when setting up a security system for the bank. VIVOTEK is honoured to cooperate with a local partner, and provide high-level reliability and thus make the headquarters of Cosmos Bank more secure for staff, the owners, and the bank's treasured customers."

For more information, please visit: www.vivotek.com SST

Point-Of-Sale System Breaches – Threats To The Retail And Hospitality Industries

Article courtesy of David Siah, Country Manager, Singapore, Trend Micro & TrendLabs Research

PoS systems in retail and hospitality industry networks

Point-of-sale (PoS) systems have been around in one form or another for decades. Businesses in the retail and hospitality industries use these systems not only to accept payment, but to provide other operational information such as accounting, sales tracking and inventory management.

From a security perspective, the most immediate risk to businesses and customers lies in accepting payments. The information that customers hand over, if captured, can be used by cybercriminals to commit credit card fraud. Risk of exposure is the primary reason why the Payment Card Industry Security Standards Council (PCISCC) has established data security standards for organisations that handle the information of credit, debit, and ATM cardholders.

PoS systems require some sort of connection to a network in order to contact external credit card processors. This is necessary in order to validate credit card transactions. How this connection is provided may depend on the store in question.

However, large businesses that wish to tie their PoS with other back-end systems may connect the former to their own internal networks. In addition, in order to reduce costs and simplify administration and maintenance, PoS machines may be remotely managed over these internal networks.

Many PoS terminals are built using embedded versions of Microsoft Windows. This means that it is trivial for an attacker to create and develop

malware that would run on a PoS terminal, if he can gain access to that terminal and bypass or defeat any running security solutions present.

Sufficiently skilled and determined attackers can thus go after a business's PoS terminals on a large scale and compromise the credit cards of thousands of users at a time. The same network connectivity can also be leveraged to help exfiltrate any stolen information.

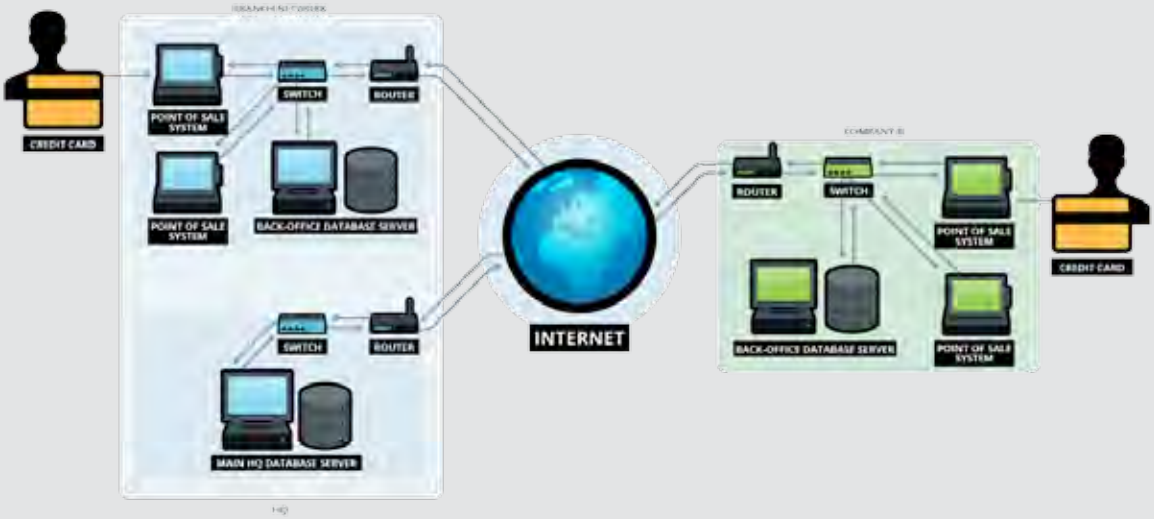


Figure 1: A basic network setup for PoS systems

PoS device and network setup weaknesses

PoS systems are difficult to secure, mostly because of their role and exposed location in the network. They handle critical information and at the same time require being managed from remote locations, a scenario typical of corporate environments that implement software package management solutions.

Industry-established standards such as the PCI Data Security Standard (DSS) are set up to ensure that the systems – and the information they handle – remain safe from unauthorised access. However it only takes one weakness to infiltrate a network.

Hacking PoS devices

A PoS device can be considered the most important landmark in any retail location, as it is where all purchases are finalised. An attacker can find a way to infect a PoS device even before deployment, for instance, in the vendor's factory shop floor. There have been cases of newly purchased devices such as navigation devices, smartphones, and even MP3 players found to contain malware.

PoS devices are normally "guarded" by an employee during operating hours so getting to PoS device and infecting it with malware can prove difficult for an attacker though still very much doable. All it takes is a disgruntled employee or a well-disguised attacker to gain access to a system and manually install an information-stealing malware into it. Attackers may also take advantage of "self-service" terminals and PoS locations that are not as closely monitored as other stations.

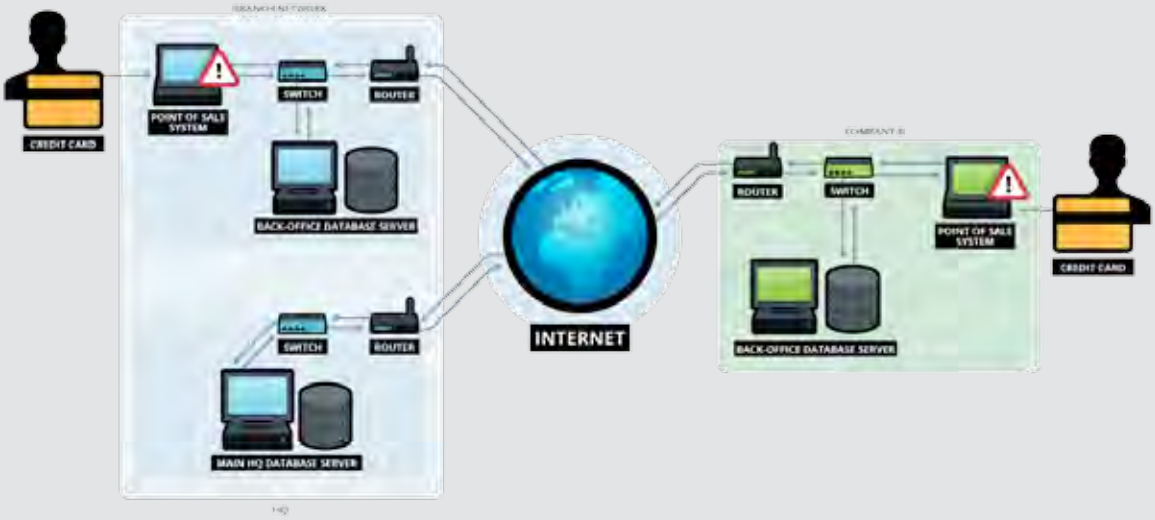


Figure 2: PoS device weaknesses

Hacking network communications

Network-level hacking is another technique seen used in the past wherein attackers may try to check for access to the PoS system through the network that the systems belong to. This can also be made possible through different methods. One way can be through shared connections between systems in an establishment such as PoS systems that share the same connection with the Wi-Fi hotspot provided to consumers. These PoS systems can be using Wi-Fi such as in a "back-office" area to communicate with servers. The PoS systems can also be using a closed Wi-Fi network but attackers can still be able to crack its passphrase. Attackers can also find an open port on a switch and add their own Wi-Fi access point.

Such security holes are products of non-compliance. The security standard for payment card processing requires a secure connection for the PoS system, encryption of card data, authentication for remote access to and from PoS machines, and many other methods that ensure that transactions remain safe from unauthorised access.

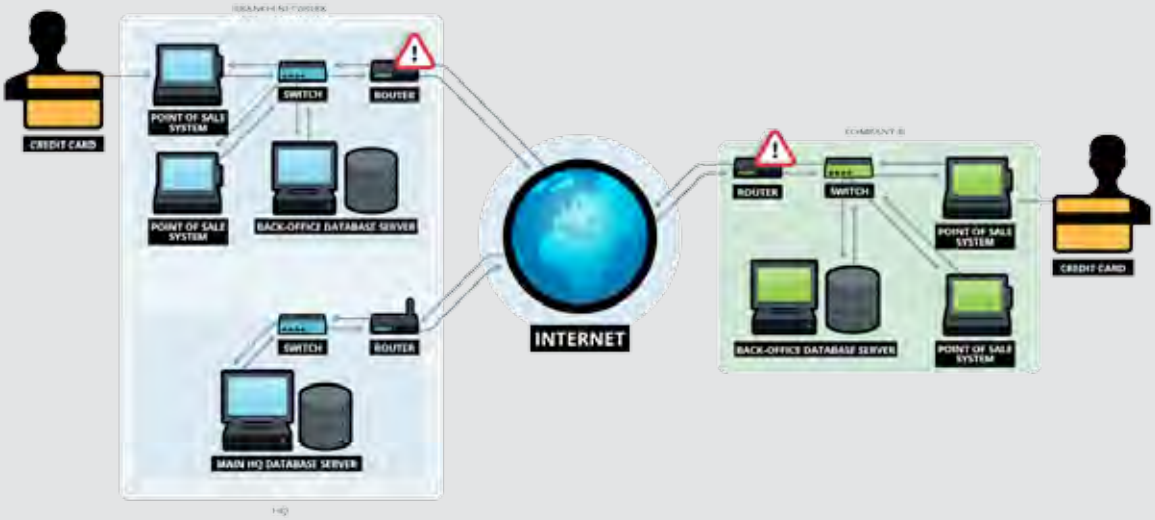


Figure 3: Network-level hacking

Targeting specific servers

Infiltrating networks is possibly the most sophisticated method an attacker can use in order to get in to a PoS device but it also promises the biggest payout. Unlike device and network-level infiltration, a successful server breach will give attackers access to not just a single PoS system or a network of PoS systems in a single location, but depending on the architecture, possibly all PoS systems controlled by the retailer in multiple locations. This is not without additional difficulties, however, as they need to gain network access before they can reach the servers. It may also take some work for attackers to know the available software on the server and the means to exploit it.

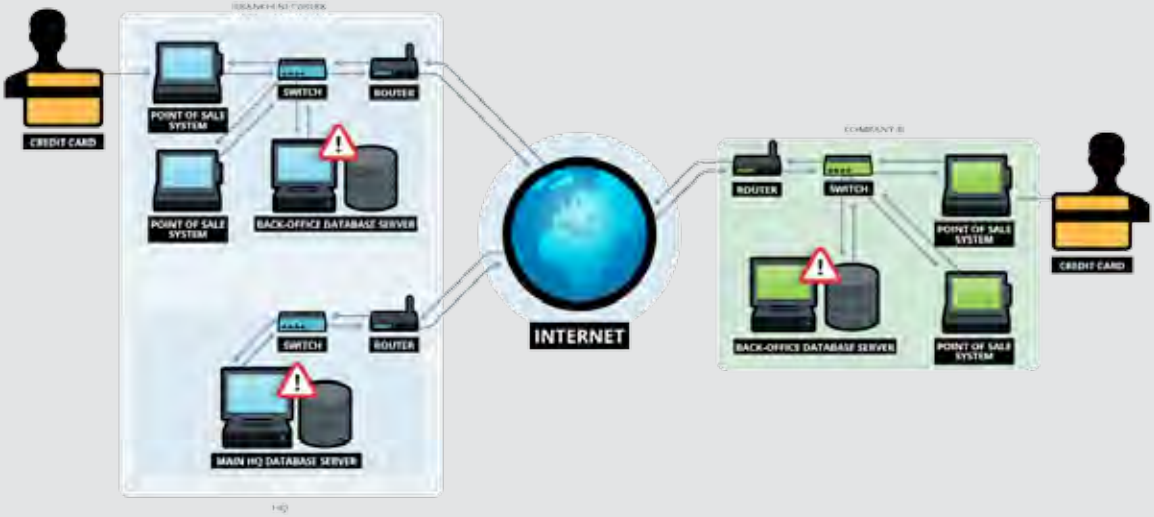


Figure 4: Hacking into back-end office systems

Point of entry and lateral movement in a network

In a typical attack, a target receives a socially engineered message such as an email or an instant message that encourages him to click a link or open a file. The links and files sent by attackers contain a piece of malware that exploits vulnerabilities in popular software such as Adobe Reader (e.g. PDF files) and Microsoft office (e.g. Doc files). They may also send .EXE files that come with false icons and file name extensions. The payload of these exploits is a piece of malware that is silently executed on the target's computer. This allows the attackers to take control of and obtain data from the compromised computer, ultimately establishing the beachhead.

They typically download remote access Trojans or tools that allow them to execute shell commands in real-time on the compromised host. In addition, they may seek to elevate their privileges that they could then use in techniques such as "pass-the-hash" and seek out key targets. In this particular scenario, the key target may be a system that will allow the attacker to deploy malware to all PoS systems within the network.

As the attackers move throughout the target's network, they explore and collect information that can be used in future attacks or prepared for ex-filtration. They may also set up additional back doors in case the others are discovered.

Find an updated mechanism to deploy malware on a large scale

A server-level attack may involve the misuse of any management system used by the retailer to monitor or maintain all PoS systems. It may be one to manage system updates, collect accounting data from branches, or even one that

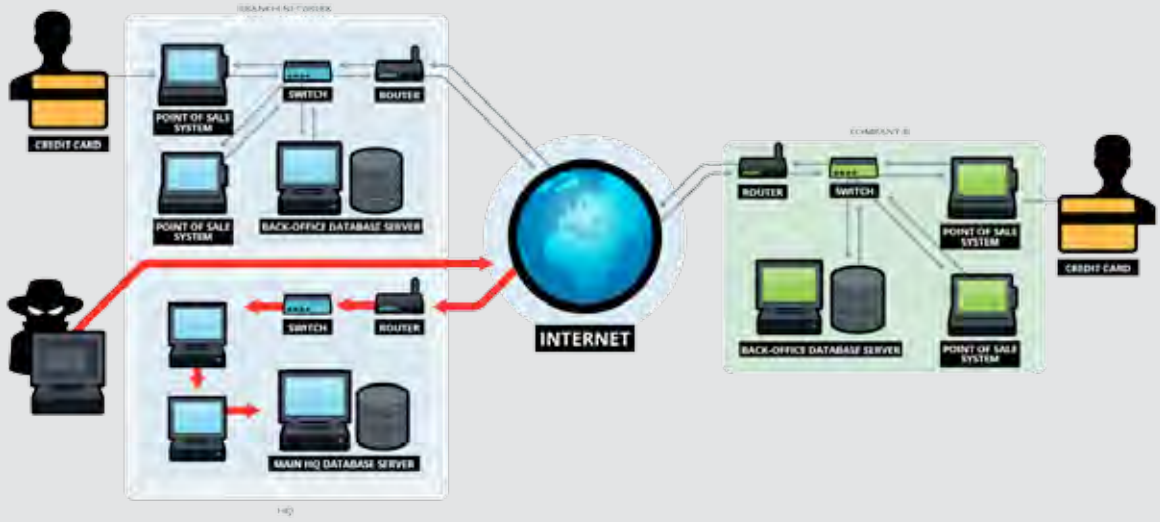


Figure 5: Point of entry and lateral movement

monitors the man-hours employees put in. Any system that has control or access to all PoS systems is a potential target for attackers that aim for a server-level infiltration.

Once attackers gain access to this system, they gain access to the entire network of PoS systems, and are enabled to deploy malware that will steal customer information.

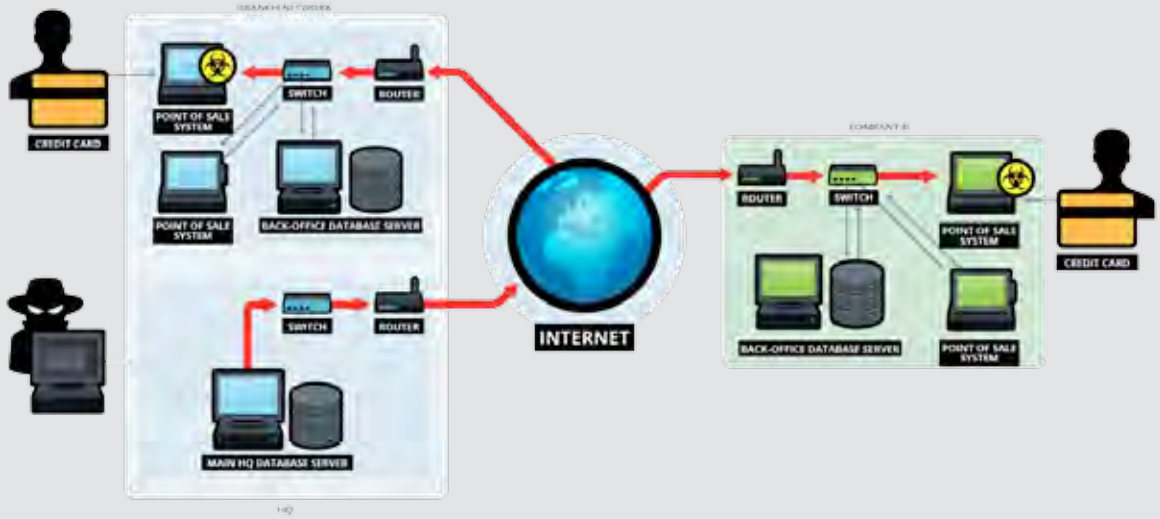


Figure 6: Spreading PoS malware to devices

Data exfiltration

After the malware is installed on the PoS systems and the information is stolen, the next critical step for attackers is to get the stolen data from the target's infrastructure and under their control. In order to accomplish this objective without getting caught, the attackers will use a variety of techniques to obfuscate their activities. They can, for instance, collect

and compress the desired data then split the compressed file into chunks that can be transmitted to locations under their control. A variety of transmission methods are used such as File Transfer Protocol (FTP) and HTTP. Attackers can, however, also use methods such as exfiltrating data by using and abusing the Tor anonymity network.

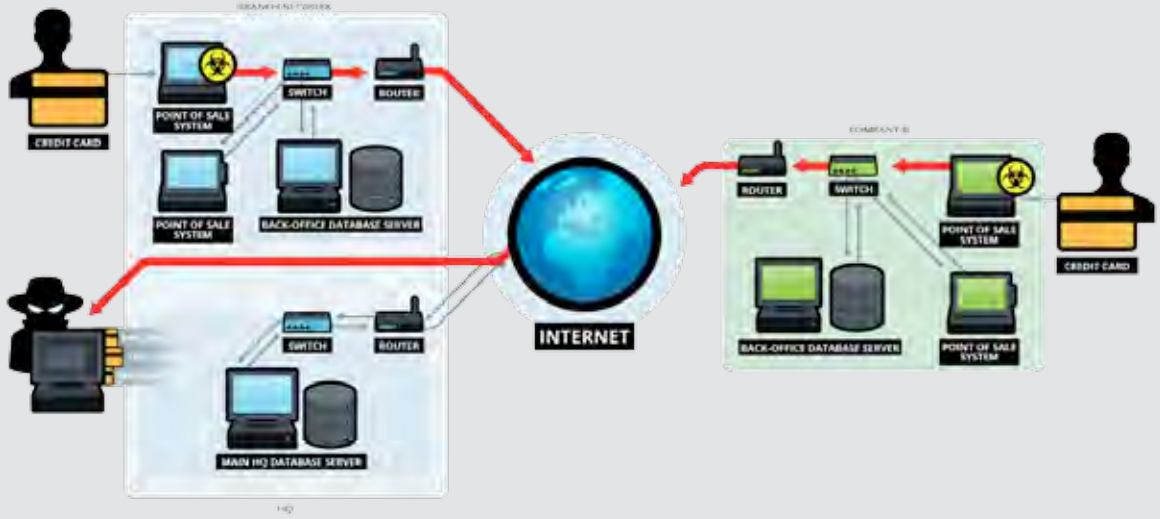
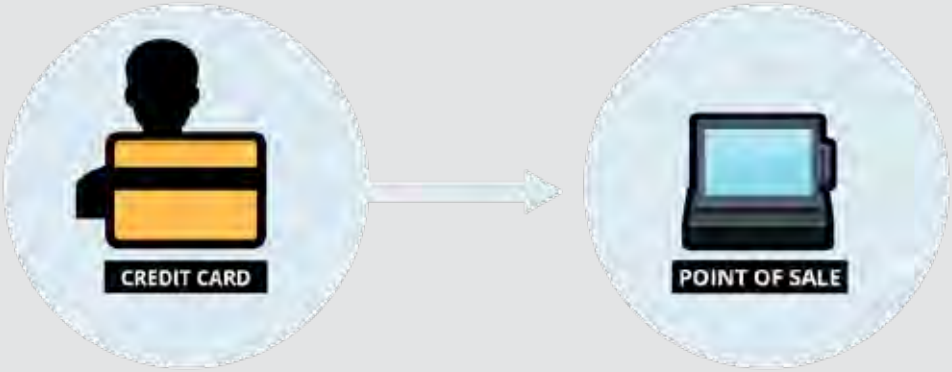


Figure 7: Spreading PoS malware to devices

Common PoS device malware and how they scrape and send credit card information back to attackers

To comply with the PCI DSS requirements, the payment card industry uses a set of security standards that enforce end-to-end encryption of sensitive payment data captured from payment cards when this data is transmitted, received or stored. However, when the information is first read from the card, it can be found inside the PoS device's memory in unencrypted form. PoS malware exploit this by capturing the payment card information directly from the memory; this behaviour is known as "RAM scraping".



Several malware families that target PoS devices are known to exist in the wild. These families are all widely available in underground marketplaces and have been used in various attacks.

vSkimmer

The vSkimmer malware family is easy to obtain for cybercriminals, as a cracked builder and control panel is readily available. As is the case with most information-stealing malware, it uploads any data it captures to its own C&C server. However, if it does not find its server, it has another data exfiltration method. It checks for the presence of a removable drive with the label "KARTOXA007." If this drive is found, it drops a file that contains any stolen information into it, allowing a method of offline data exfiltration.

We detect vSkimmer malware under the HESETOX family.

Decebel

The Decebel malware family adds well-defined evasion techniques to PoS malware.

Cybercriminals are aware that researchers are looking into this emerging threat and so are accordingly designing their wares. Decebel checks if sandboxing or analysis tools are present on a machine before running. This aims to make detection and analysis more difficult, buying attackers more time before their scheme is eventually discovered and shut down.

As is the case with other PoS malware families, Decebel uploads stolen information to its C&C server via HTTP POST. This family is detected as DECBAL.

BlackPOS

BlackPOS, also known as the "Memory Form Grabber," is the most well known PoS malware family. Like all PoS malware, BlackPOS checks the PoS terminal's memory for sensitive information to steal. However, even here, BlackPOS shows some sophistication, as some variants are only set to carry out information theft between 10 a.m. and 5 p.m. any stolen information is stored in a .TXT or .DLL file, depending on the variant.

Unlike other malware families that directly upload stolen information to a C&C server, BlackPOS uses FTP to upload information to a server of the attackers' choosing. This allows attackers to consolidate stolen data from multiple PoS terminals on a single server, allowing for more control over data exfiltration.

Associated Threats

PoS malware are rarely, if ever, used without other malware to help carry out attacks. It is worth noting that PoS malware are almost never used on its own. Other malware components are frequently used to carry out PoS attacks.

Shellcode-loading malware may also be used in a PoS attack. Command and control for PoS malware is difficult, as again communications to an external server may not be possible. Instead, a compromised server inside the network acts as a C&C server.

This C&C server sends shellcode across the network to PoS machines where they are loaded and executed on affected machines. This allows for covert command-and-control and renders forensic investigation of any attack more difficult.

Impact of PoS hacks to the industry and consumer

A major effect of PoS hacks would be the possibility of identity theft. Personal and sensitive information stolen from credit and debit cards can be used to impersonate unsuspecting consumers.These victims may soon encounter problems such as fraudulent purchases, financial loss, and damaged credit standing. Trend Micro's research into different cybercriminal underground forums has revealed an on going, thriving and organised economy of buyers and sellers of stolen information.

Compromised banks and retailers may experience backlash from PoS hacks. The public may opt to turn to other banks and retailers. Such breaches may also lead to class-action lawsuits. Compromised organisations may also find their value dropping, if they are publicly traded.

What should consumers do?

While consumers cannot control whether or not their favourite business establishments are secured against the threats of PoS malware, they can take some steps to ensure that their accounts are not put at unnecessary risk.

Reputable merchants will inform users about any potential breaches as well as absorb any financial losses as a direct result of the fraud. However, users may be defrauded even before merchants become aware of any problem so they should be on guard in any case.

Check Your Bank and Credit/Debit Card Statements

Users should regularly check their bank statements for any anomalous transactions. Online banking sites allow users to check recent transactions. Going over this list on a regular basis should allow users to spot and dispute fraudulent transactions made on their cards.

Ask for a Chip-and-PIN Card

In many countries, both banks and retailers have shifted to using "chip-and-personal identification number (PIN)" or Europay, MasterCard, and Visa (EMV) cards, which primarily use an embedded chip to hold the information on the credit card instead of a magnetic strip.

EMV cards offer improved security over conventional magnetic strip cards. However, not all banks offer EMV cards to all of their customers. In these cases, users should check with their banks if EMV cards are available.

Minimising potential PoS system breaches

How to secure PoS devices?

- Implement hardware-based point-to-point encryption
- Limit access to the internet
- Routinely delete cardholder data
- Deploy the latest version of operating systems with updated patches
- Employ white listing in order to lock PoS systems down only to its intended uses
- Enforce policies regarding the physical repair and/or upgrade of the PoS device
- Deploy security software and keep it updated with the latest signatures
- Implement a breach detection system in the network.
- Patch the systems regularly.

How to secure networks?

Having a cloud and data centre security solutions for the retail and hospitality industries would be one way. In a retail/hospitality environment, there are many potential attack vectors to consider with the increasing number of interaction channels for customers such as websites, PoS systems, mobile apps, and social media. There are multiple security controls required in order to cover attack vendors, including controls for your applications, servers and networks. These include web applications and servers.

At Trend Micro, they recommend the following controls in one's data centre:

- Restrict communication in and out of your environment to only what is required
- Ensure that one is constantly protected against vulnerabilities in both systems and applications

- Identify when a system component has changed
- Encrypt communication between applications and data
- Continuously scan web applications for potential vulnerabilities

To address risks within your evolving data centre, Trend Micro provides a security solution that is open, automated, and highly scalable, that fits your existing infrastructure, seamlessly integrating with key environments such as VMware or cloud environments such as Amazon Web Services.

Changes in system components can occur for many reasons, many of which are not due to an attack against your system. That said, monitoring systems such as PoS devices for changes is becoming more and more critical to your security controls. It can not only provide an early indication of a problem, it is actually required by various compliance standards such as the PCI DSS.

Trend Micro *Deep Security* offers File Integrity Monitoring capabilities to monitor critical OS and application files such as directories, registry keys, and values to detect and report malicious and unexpected changes in real time. These include changes to PoS systems.

Deep Security can restrict communication in and out of your environment through a firewall policy that can be tailored for specific server requirements and protect against both inbound and outbound communication. Its firewall capabilities offer logging and alerting to make it easier to troubleshoot and manage.

With your business demanding a constantly evolving application use, it is often difficult to keep up with patching systems against known vulnerabilities. This is where *Deep Security Intrusion Prevention* capabilities that protect against potential exploits on vulnerabilities are important to have on the list. An important capability of our intrusion prevention is the ability to automatically update security policies to ensure the right protection is applied, even before you have had a chance to patch.

Finally, *Deep Security Anti-Malware* that includes Web reputation detection will not only protect against malware but also detects and protects against known malicious URLs.

When those applications are available through the Web and provide customers, partners, or global employees the ability to share information, detection of potential threats or occasional penetration testing is not enough, especially as the number of apps increases. Trend Micro offers *Deep Security* for Web Apps, a comprehensive, integrated software-as-a-service (SaaS) offering that continuously detects vulnerabilities, delivers actionable security insight, and protects applications with Secure Sockets Layer (SSL) certificates to encrypt transactions and communications, as well as Intrusion Prevention and Web Application Firewall (WAF) rules.

What to check for in a third-party vendor agreement?

In several cases, businesses may opt to outsource their payment processing function. This presents an additional layer that can be found vulnerable to exposure. Therefore, organisations must make sure that vendors are contractually bound to comply with their security-related requirements.

The agreement must cover how customer data is captured, stored, processed, and transmitted, including baseline compliance requirements such as to the PCI DSS. For instance, the contract must require encryption in all stages of transmitting data. It may also set forth requiring background checks on employees with access to customer information databases.

The agreement must also clearly outline who is the person of contact for service and support escalation when anomalies and security incidents arise. Anticipating various security breach scenarios is key to coming up with third-party outsourcing agreements that indicate responsibilities, accountabilities, liability limitations, or grounds for declaring a breach of contract.

For more information, please visit: www.trendmicro.com SST

Magnifying On The Northeast Asia Security Climate

Information contributors:

Anmol Singh, Principle Research Analyst from Gartner

Peter Francis, Vice President of EMEA & Asia from Gallagher

Elyse Wang, Business Development Manager from Antaira Technologies

Introduction

Security analysts at Transparency Market Research have studied that on a global scale, the physical security market was initially valued at USD 48.05 billion 3 to 4 years back. However the market is expected to more than double its numbers to USD 125.03 billion by time it reaches 2019, growing at a Compound Annual Growth Rate (CAGR) of 14.9 per cent.

Not surprisingly, the consistent growing demand for security stems from the very circumstance of globalisation and nations being exposed to the likelihood of vast global issues like terrorism and other major crime undertakings. Due to these factors, governments have begun to pay more attention to upping their yearly budget, allocated for higher-tiered security.

Anmol Singh, Principle Research Analyst from Gartner analyses that, "The security market in Asia Pacific has been expanding by leaps and bounds over the last decade. In recent years, this rapid growth is mainly fuelled by the emergence of digital business initiatives and Internet of Things (IoT), which has brought significant changes in technology products and services used to protect organisations, from cloud computing to application development, from cyber security to risk management."

The Northeast Asia region comprises of many multifaceted and delicate nations within the global security landscape. We take a look at an industry that has such a common foundation everywhere around the world yet each nation has individual expectations and rate at embracing latest security technologies and systems.

The security trends - 2016 onwards

Singh determines that in the Northeast Asia region, "Hong Kong is amongst the front runners in adopting the latest security trends in the banking and financial services industry, with Japan and South Korea being the early adopters of some new security technologies in other verticals such as the manufacturing and healthcare industry."

Implementation of online platforms comprising of security technologies has been a norm amongst organisations. It has by far made security management more cost saving and systematic. Peter Francis, Vice President of EMEA & Asia from Gallagher foresees that there will be more upcoming trends of Smart Cities in the Northeast region of Asia. "From the security aspect, the situational awareness software platform is the solutions trend. It allows all sub-systems to integrate together and help the operator respond faster, more accurately and with prompt actions – therefore minimising faults", Francis says.

Trends begin because some organisation, somewhere requires a security platform that ensures a holistic approach and solution to their problems. Thus, security trends are often started by ensuring that the needs of solutions seekers are met and what they require and ask for are catered to. Francis echoes this notion whilst explaining that, "At Gallagher, inspiration for the development of new products comes from our customers. We are constantly looking closely at industry trends as we hold a strong believe that this is the best way to ensure we meet the future needs of our customers. For instance, Gallagher foresee mobile applications becoming one of the latest security trends in Northeast Asia."

Francis continues, "As a result our teams have taken the initiative to develop our Mobile Client Application and the new Mobile Reader for Apple Devices. It is a significant trend because it is one that most people can utilise. Mobile apps are invaluable to help security managers monitor and maintain their security systems from anywhere at any time either by Wifi, cellular, network or Internet."

Elyse Wang, Business Development Manager from Antaira Technologies also shares her forecasts and feels that when it comes to growing security trends in the Northeast Asia region, "Wireless devices and the IoT are gaining speed and popularity within the region. Japan however, has its own features about the IoT because of their high development of technology and dense elderly population. In Japan, 25 per cent of their population is aged over 65. Therefore health data tracking in smart home plays an important role in order to monitor health condition and help respond to emergencies."

Northeast Asia is a huge part of the ASEAN region and therefore trends are most likely to follow-up in other parts of Asia as well. Influences from nearby countries will definitely have its impacts on local trends. However, having said that, different countries have different needs and the pace at which these trends are embrace may also differ. Francis adds, "Bluetooth low energy technology is another trend taking off. The technology applies to wireless door locks and card readers allowing a cardholder to unlock the door within a 10 metre range when approaching it."

The revolving door to the developments in the security arena in Northeast Asia

Security has very much evolved throughout the decades, in accordance to what technology has to offer the industry. The security market has indeed transformed and diversified over the last few years in the North-Eastern part of Asia and at the same time provided security solutions seekers with more convenience and options for their desired solutions and its implementation.

In agreement with the above statement is Francis as he justifies, "Most of the security systems today in the Northeast Asia regions are now required to be TCP/IP Network/Internet/Cloud based operations. A significant level of requirement has developed over the past few decades for security operators to have a greater level of IT knowledge. What was taught and learnt in the past for security systems are no longer parallel and sufficient to what is required upon current standards to efficiently manage today's systems. We are able to see the decision making within organisations already switching from company administration to the IT department as technology continues to improve and guide the way we run our businesses."

Singh echoes Francis' sentiments saying that, "Organisations in the Northeast Asia region, especially those in asset-intensive industries like manufacturing or utilities, have operational technology (OT) systems from equipment manufacturers that are moving from proprietary communications and networks to Internet Protocol (IP)-based technologies. More enterprise assets are being automated by OT systems based on commercial software products with embedded software assets that need to be managed, secured and provisioned for enterprise-class use. OT is the industrial subset of the IoT, and will include billions of interconnected sensors and systems, many of which will communicate without human involvement, yet will need to be protected and secured."

Additionally, Wang says, "The security outlook in Northeast Asia is moving forth towards digitisation, networking and smart cities, and integrating the three areas together." This is the time where the Internet is required more than ever. It has taken over the world of security and given people a new perspective to having a tighter yet more convenient form of security within a premise.

Monitoring the swift shifts in the security world, Singh says, "Changes in mainstream IT and digital business imperatives brought by mobile and cloud computing, social media and big data have resulted in demands for sophisticated analytics and rapid response to digital security needs in Northeast Asia. The digital explosion on a global scale affecting vertical markets that use industrial automation and control technologies, sometime referred to as operational technology (OT), such as automotive manufacturing, energy and utilities, transportation systems, building

automation and facilities management, digital healthcare and even smart home solutions – will dominate the development and implementation of security technology and solutions throughout 2016 in Northeast Asia."

There is much adaptation to look forward to in the security world in the Northeast Asia region, mainly in Taiwan, Japan and Hong Kong. Wang mentions that Korea is a nation that has to abide by strict rules and regulations by the government on security equipment imports, "Korea protects their domestic industries greatly. They however have a great amount of demand on military and homeland security."

Security entities and its functions are no longer limited to just having a physical individual mending a particular security booth. Francis believes that, "The cloud based architecture solution, Software as a Services (SaaS), could significantly impact the market here by not only reducing the manpower needed by guarding services but also allowing operators to access a simplified and unified system software from anywhere in the world through a web browser. However higher network and IT security is still required for both the private cloud and global and cloud architecture solutions."

In conclusion

Security trends and up-keeps in the Northeast Asia region are very much influenced by security on a global scale. Every product, system and technology in the security market are interconnected. Singh rationalises that, "IT, operational technology (OT), the Internet of Things (IoT) and physical security technologies will have interdependencies that require a risk-based approach to governance and management. Digital risk management will be the next evolution in enterprise risk and security for digital businesses by expanding the scope of technologies protected."

Observing and studying the security market in this particular region, Singh says, "Enterprises have traditionally been overly dependent on blocking and prevention mechanisms that are decreasingly effective against advanced attacks. Comprehensive protection requires an adaptive protection process integrating predictive, preventive, detective and responsive capabilities."

He adds-on, "To achieve that, organisations can consider shifting the security mind-set from "incident response" to "continuous response", adopting an adaptive security architecture protection from advanced threats, developing a security operations centre that supports continuous monitoring and is responsible for the continuous threat protection process and more."

The security picture is now a bigger realm, with solution seekers wanting functionality and productivity elements thrown into the decision-making factor. Security management can be a tricky responsibility and according to Singh, "By 2020, 60 per cent of enterprise information security budgets will be allocated to rapid detection and response approaches – up from less than 10 per cent in 2014."

Singh concludes that, "In 2015, we are seeing toughened privacy regimes and the increasing maturity in regulations. However, as the regulators work to enhance the consistencies with laws and regulations in the region, the relatively immature and underdeveloped multi-lateral response to advanced threats and transnational cybercrime remains a major challenge in the Northeast Asia region as well as around the world." SST

Axis Cameras Deliver Loss Prevention Benefits To Global Retailer Paul Smith

Introduction

Fast-growing retailer and fashion designer Paul Smith needed to replace an aging and failing legacy analogue-based CCTV camera estate located in its 45 stores around the world. Paul Smith's IT department therefore took over the management of the legacy cameras with a view to upgrading the whole system to IP video, over a three year period.

Mission

To meet its targets, Paul Smith needed a system that was capable of lasting at least 10 years. Therefore it required

a network camera manufacturer, which had global support capability, as well as retail sector expertise and a strong focus on research and development to future-proof the new investment.

Solution

After a painstaking evaluation process, Paul Smith selected Axis network cameras. The company specified AXIS M3014 Network Cameras in all stores, as part of the complete IP video upgrade, with most stores fitted with 8 to 12 cameras. Additionally, storerooms of some outlets were equipped with AXIS M3005-V Network Cameras. The end of the 3-year IP video upgrade programme would have installed a total of over 550 cameras in 2015.

Six stores with known loss prevention issues were earmarked for a hybrid CCTV-IP solution to help deliver rapid results. In these stores AXIS Q7406 Video Encoder Blades were fitted into existing local CCTV servers, enabling current CCTV cameras to be integrated into Paul Smith's new IP-based video surveillance system. 64 analogue cameras have so far been brought onto the network in this way.

Result

Paul Smith is replacing an aging and unmanageable CCTV estate with a state-of-the-art IP video system. This provides 100 per cent storewide coverage and HDTV 720p images in all its fully owned stores globally. AXIS M3014 is designed to fit into the same size ceiling void as a standard spotlight and is so discreet that it is often mistaken for

a spotlight rather than a powerful HDTV network camera. Paul Smith is able to gather high quality images capable of use as evidence in a court of law. In the future it will also provide a platform to integrate video analytics software for dwell-time analysis, heat mapping, people counting, facial recognition and even CRM and Point of Sale systems integration.

Centrally managed and future-proofed global network video

Paul Smith is one of the UK's leading retail and fashion success stories with major offices and showrooms in the key fashion centres of the world, including London, Milan, New York, Paris, Amsterdam, Antwerp, Düsseldorf, Sydney and a significant retail presence in 35 countries worldwide. It currently has 24 stores in the UK. The company's growth in the US and across Europe is accelerating with plans to open at least five new stores every year for the next five years. The business has annual sales exceeding £400 million today. Founder Sir Paul Smith opened his first shop in his native Nottingham at the age of 24 in 1970 and has now established himself as the pre-eminent British fashion designer.

Paul Smith's Head of IT, Lee Bingham, looks for IP-based solutions, which are capable of scaling quickly and effectively and can be managed within the corporate network. To simplify management and bring down costs he only specifies new IT devices and services, which will last at least 10 years.

Paul Smith's legacy CCTV estate had grown organically as the group expanded around the world. When the IT department was asked to take over the running of the CCTV systems, Bingham insisted that it must be moved to IP, "If it is not IP then it is not IT, and therefore it made no sense to move its management from our Facilities Management team over to the IT department un- less images were going to be accessible on the network by authorised managers from their desktops."

Paul Smith's IT department researched the market, looking for robust, scalable IP video hardware and software. After a comprehensive evaluation Paul Smith chose Axis network cameras, together with Axis video encoders to integrate some of those existing CCTV cameras not being immediately replaced. Axis network cameras deliver images, which are recorded on new local servers using Milestone XProtect

Corporate Video Management Software. The installation and networking of the new IP video system in 45 stores globally will take three years and is being carried out by Axis Partner A1 Data Communications.

Bingham said, "Just days after the Axis cameras were installed in Paul Smith's new store in Beak Street, London, someone bought goods there with a fraudulent US-based credit card. Because the card was not 'Chip and Pin' that person was able to complete the transaction but when we were alerted by the bank that this was fraudulent we were able to refer to the new system's HDTV quality images to identify the suspect, showing the fraudulent transaction in progress and then hand the evidence to the authorities."

"Our objective, as soon as the new IP video system has been rolled out globally, will be to build on this investment by extending its value beyond loss prevention. We will work closely with our retail management team to explore the power of the new system - potentially deploying techniques such as facial recognition, heat mapping and dwell-time analytics that enable us to better understand and serve our customers", Bingham continued.

The new IP video system provides a cost effective platform for integrating facial recognition capabilities. Applications can be uploaded to local cameras, enabling managers to measure the time customers are spending interacting with a new line of clothing or getting advice from staff. Facial recognition can also be used to detect and alert store managers if known shoplifters or fraudsters enter the store.

Lee Bingham concludes saying, "We see specific value in knowing our best customers wherever we are serving them. We want our best online customers to be recognised as such when they come into store. There would be some logic in being able to integrate our CRM system with an IP video-based facial recognition system to ensure high value customers have the best possible experience in store. Additionally, we know video analytics can be used to study how customers walk through a store. Heat mapping and dwell-time analytics software could be used to analyse which displays are working best to attract and retain shoppers. Managers can use this business intelligence to investigate further and make improvements. It is this sort of capability that we will be looking to offer to managers in the coming years."

For more information, please visit: www.axis.com SST

BT Inbound Contact Global Makes Agoda Always Accessible

Introduction

When your business is web-based you could be located anywhere. That is what being virtual is all about. But for telephone support, it is a great competitive advantage to look local and Arjan van der Meer Director of IT operations of Bangkok-based Agoda did not want people paying international rates for customer service.

Now, with Inbound Contact global from BT Global Services, people are able to call Agoda on local phone numbers in their own country. They are answered 24/7 in their own language. Yet they have no idea that they are talking to someone in any of 22 Agoda offices worldwide. So Arjan cracked the problem of being here, there and everywhere else – all at the same time.

Challenge

As one of the new breed of internet-only businesses, everyone is a potential Agoda customer. Part of the Priceline Group, Agoda is Asia's leading online hotel reservations business. A self-service model – using the Agoda website, smartphone applications or social media – matches customer accommodation requests to an inventory of over 170, 000 hotels worldwide. Headquartered in Bangkok and with offices in 22 major cities the company is expanding fast, with triple-digit, year-on-year growth.

Each transaction initially uses advanced web technologies to ensure a speedy reservation process. Once customers have made a booking they are provided with a phone number for enquiries so that if they have a question or need to change their plans they can talk to someone.

Arjan van der Meer explains, "We are expanding rapidly into Europe, the Middle East and the Americas, and assuring great customer service on a global scale demands smart technology."

Solution

Three Agoda contact centres – in Bangkok, Kuala Lumpur and Budapest – provide a virtual worldwide presence. Equipped with state-of-the-art technology, they offer service in 11 languages between them. The problem was cost effectively routing calls originating from anywhere in the world to that powerful CRM resource.

Arjan van der Meer says, "We needed an associate who could offer a consistent class-leading network service, independent of location, virtually anywhere in the world. BT Global Services was the clear choice."

BT provided an Inbound Contact global solution, which works with an interactive voice response (IVR) platform and enables intelligent call routing. Customers call one of 34 local numbers in 21 different countries, apparently using a local service. When the call hits the BT Global

Services network, it is routed to the first free agent best qualified to answer the query. The routing pattern was pre-configured by Agoda to take account, for example, of availability of destinations.

The call is then routed to the appropriate Agoda contact centre via a global Agoda data centre (of which there are several spread across multiple continents). This is all transparent to the customer and there is no noticeable delay. The minority of calls that cannot be resolved by IVR are routed direct to a contact centre with the right agent availability and skillset, based upon originating time zone and language.

Local support for the Agoda IT team in Bangkok was essential, and BT has a network of solution partners around the world. Infonet Thailand, the BT Alliance partner in Bangkok, supports Agoda on a daily basis with activities like activating new numbers, online reporting and billing.

Saran Snongjati, Director of Global Services for Infonet Thailand, explains, "The BT partnership model allows Infonet Thailand to provide customers with world-class global network services, while offering local language support. It is a very compelling proposition. Combining our strengths truly brings together the best of both worlds."

Conclusion

Since the rollout of the global service Agoda is efficiently dealing with thousands of calls each day. Scalability is built in - an important consideration given that call volumes are set to double within a matter of months.

The BT architecture allows calls to be distributed evenly across all three call centres. This enables workload balancing, and optimises agent utilisation and efficiency.

Call volumes and agent performance can be analysed using BT management software, and operational changes made if needed.

Business resilience is enhanced too. Arjan van der Meer says: "Political unrest or natural disasters can happen out of the blue in any country. BT is able to switch voice traffic to alternative locations should agents be denied access to their contact centres for any reason."

BT uses its relationships with local service providers to blend calls from any location into a single end-to-end solution. "Complexity is reduced," concludes Arjan van der Meer, "and it is because we work with BT as a single global communications partner, rather than having the administrative nightmare of dealing with multiple in-country service providers."

For more information, please visit: http://home.bt.com/ SST

Dahua Provides Patented HDCVI Technology To Secure Lulu Mall In Oman

Introduction

Lulu Hypermarket in Muscat, Oman, is a hypermarket chain and retail venture started by Lulu Group International in 2000. It has over 30, 000 employees of various nationalities. Lulu Hypermarket is one of the largest retail chains in Asia and is the biggest in Middle East with 115 outlets in the Gulf Cooperation Council (GCC) countries and one in Kochi, Kerala, India. It is amongst the world's 50 fastest growing retailers according to research firm, Deloitte.

Solution

Dahua provided HDCVI technology to secure the branch of Lulu Hypermarket in Muscat with cooperation with its system integrator China Communications Services. This is the first time that Dahua and China Communications Services have cooperated for an entire CCTV project. Both of their extensive experience in CCTV resulted in a smooth and successful implementation for Lulu.

Lulu mainly used Dahua HDCVI Professional series products, including HDCVI cameras, HDCVI DVRs, VMS, IP storage, video wall and more. Dahua provided around 250 cameras, which includes all three types, bullet, dome and PTZ. A video wall display unit were also used in the control centre and IP SAN storage devices are used to meet 90 days recording requirements.

Dahua HDCVI Professional series adopts the patented DH5000 chipset and high performance CMOS sensor. The camera retains the ease-of-use of an analog system while offering up to 1080P HD video output. Pro series is suitable for the users who want to secure small and medium scale applications like airports, hospitals, schools, upscale hotels or banks.

"HDCVI is Dahua patented technology featuring HD analog video transmission over coaxial cable, allowing reliable long-distance HD transmission at lower cost. As for the Lulu Hypermarket, we provided our HDCVI professional series products to protect the whole market," said Rio Mao, Sales Director of APAC at Dahua Technology. "Dahua appreciated the teamwork with China Communications Services, which made the project successful and was happily accepted by Lulu Hypermarket. We are obviously looking for further cooperation with China Communications Services for more projects."

"We really appreciate this great support from Dahua, and we have more confidence to work with Dahua together again, in the whole Middle East market," said Zhu Linghua, Manager of Overseas Department of China Communications Services. "I believe we can achieve more mutually beneficial project starts from this successful case, and continue cooperation with each other in the near future."

For more information, please visit: www.dahuasecurity.com SST

Marc O'Polo Chooses Nedap's uPASS Access For Convenient Hands-Free Access

Introduction

The premium modern casual brand Marc O'Polo in Stephanskirchen has successfully implemented an access control system. The system provides Marc O'Polo with a tailor-made solution suitable for a variety of requirements. Nedap's uPASS Access readers for convenient hands-free access, developed by Nedap Identification Systems, plays an important role is this access control solution.

On a daily basis, over 600 employees enter and leave the premises at the headquarters of Marc O'Polo in Stephanskirchen. Steady growth over recent years made it necessary to improve the process of access control. Marc O'Polo wanted a user-friendly system to prevent people from accessing the premises unauthorised, without causing inconvenience for employees.

Flexible working hours, flexible system

Flexible and varied working hours called for a solution at Marc O'Polo that gave employees the greatest possible freedom of movement. Convenient, fast, uncomplicated – Nedap's uPASS Access meets these criteria while remaining in the background.

Fashion accessory

As a fashion brand, Marc O'Polo had its own requirements when it came to the design of employee ID cards. Potential solutions for feasibility, aesthetics, practicality and design were discussed and tested in consultation with the management and various departments. For Marc O'Polo two access cards are developed - one for employees and one for visitors. The look of the cards matches with the corporate identity and the requirements of a modern premium casual brand, and is clearly showing the company to whom the card belongs. Attached to a quality leather strap, the security cards look like an everyday fashion accessory.

Hands-free access reader

Nedap's uPASS Access is the world's smallest UHF reader for hands-free access to secured buildings, sections and rooms. This groundbreaking reader can read access badges at distances of up to 2 meters. It is specifically designed for doorpost mounting and is the perfect solution for entrances that require both convenience and security, like office buildings, retail shops, hospitals, clean rooms and entries for disabled persons. This ultra-small reader utilises passive UHF cards (EPC GEN 2) and supports all common security industry standards.

For more information, please visit: http://www.nedapidentification.com/ SST

7-11 Philippines Upgrades Its Security with GKB HD Analog Cameras

Introduction

7-11 is one of the top-scale convenience stores with over thousand stores in Philippines. Being the world-famous convenience store, 7-11 Philippines continues to live its vision of providing consumers easy and quick shopping experiences by expanding its branches for emerging markets.

Challenges

Such convenience chain stores surveillance is required to be extremely stable, clear and easy to save backup recording. The major challenges for store managers to overcome are "crystal clear recording footage, easy-to-operate machines, and excellent sales service." They also require to receive events evidence in a short period of time.

Solutions

1. Fixing AHD Camera X4
   a. IP66
   b. Fixed Lens
   c.Class-A IR LED enables clear night view

2. Having coaxial or network cable
   a. One-time wiring arrangement
   b. Network cable skills can easily acquired with PC consumers

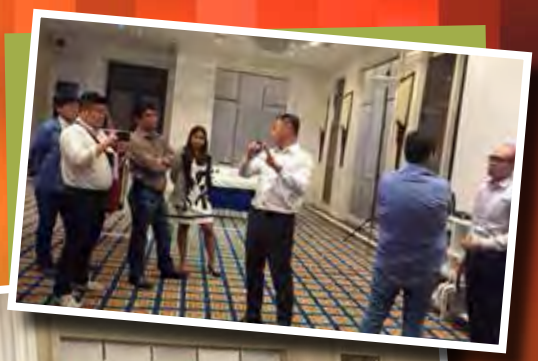
3. 4CH DVR
   a. Design without the fan
   b. Compact size
   c. DVR is able to hang on monitor to save the space

4. Ensuring there is central power supply
   a. Uninterrupted power supply
   b. Heat dissipation design

For more information, please visit: www.gkbsecurity.com SST

The Special Feature:

Checkpoint Systems



The Checkpoint Systems team & their partners

Checkpoint Systems at a glance

Checkpoint Systems is one of world's leading frontrunner in merchandising availability solutions for the retail industry – covering solutions to areas ranging from loss prevention to inventory management. Their solutions to the retail marketers derive from almost five decades of radio frequency technology expertise, market-leading RFID systems and technologies, and extensive labelling capabilities to brand, secure and track merchandise from source to shelf.

With Checkpoint's merchandise availability solutions that are tailor-fitted for the retail industry, customers can lessen the likelihood of crimes being committed within a store and aim for increased sales and profits in due course.

The innovation session in Bangkok, Thailand

Checkpoint Systems held an exclusive innovation session spanning through 2 days, meant for both their partners and customers. The event comprised of information sharing by Checkpoint's experts, product sampling and demonstration as well as an allocated time sectioned for face-to-face 'questions & answers'.

It was a well-rounded event that gave consumers and partners a peek into the world of Checkpoint Systems and their creations and inventions. While altering the façade of retail security, Checkpoint has managed to transcend the realms of obstacles faced by retailers with their Evolve E10 2.0, Evolve-Store and S3intelligent.

The Evolve E10 2.0

The Evolve E10 2.0 Deter, Deactivate, Detect

The Evolve E10 2.0 was designed to cater to the dynamic needs of the retail industry. It offers a diverse range of design options, plus an integrated visitor-counting unit and allows retailers to select the perfect solution for their present and future needs. The Evolve E10 2.0 is available in three separate technologies: Radio Frequency (RF) only, both RF and Radio Frequency Identification (RFID) or RFID only. Additionally, it supports Checkpoint's unique One Tag approach, using a single RFID tag for inventory visibility and loss prevention.

The Evolve E10 2.0 has in-built differentiated alarms based on the quantity and/or value of the merchandise leaving store and support for Checkpoint's patented Wirama Radar, which is the vastly superior tag-read accuracy, directionality and location. Checkpoint Systems also allows for Evolve E10 2.0's infinite design options – creating an antenna that will blend with individual store aesthetics and branding, ensuring that the item does not look threatening or hazardous to potential customers.

The Evolve-Store

The Evolve-Store App

The Evolve-Store in summary is a real-time App that supports real-time electronic article surveillance (EAS) and organised retail crime (ORC) event management. This was Checkpoint's solution response to retail customers' request for an easy means of ensuring that store associates leverage EAS investments appropriately while complying with store shoplifting policies and have EAS systems that are always switched on and functioning without any hiccups.

The App delivers real-time information via a smartphone or tablet, providing real-time visibility and establishes connectivity to your EAS and ORC theft prevention systems. It will also help to improve retailers conversion rates through real-time visibility of the number of shoppers in one's store and measure one's policy compliance by managing response times to alarm events. The App comprised of combined functionality of several reporting solutions and visibility of theft-related events that can affect the stores greatly.

In embracing the Evolve-Store App, the benefits of its features will intrinsically assist retail stores to make it a safe environment for their customers and help them deter opportunistic thieves and ORC activity. The App engages employees with EAS and ORC solutions and to make smarter real-time decisions without impacting sales whilst maintaining their original shrinkage reduction levels to maximise their ROI.

The S3intelligent

S3i is a smart solution that can reduce, shrink and increase on-shelf availability as well as provide critical data and analytical intelligence. S3i is a scalable wireless network that provides valuable information such as item-level locationing and inventory of merchandise on the floor, real-time event notifications and increased level of security for high-value merchandise.

S3i gives retailers the ability to openly display high-risk merchandise such as handbags, designer apparel, electronics and more. This can significantly increase the likelihood of a sale as it allows improved customer experience and secure access to the items.

These notifications can be received simultaneously via smart phones, tablets, computers, radio headsets or over a PA System. This will decrease the chances of an ORC activity going undetected.

Meeting Eddie Ang, General Manager, Asia Pacific, Channel Partners of Checkpoint Systems

With over 17 years of management experience leading sales and technical teams, Eddie Ang is the man behind overseeing relationships and operations with channel partners across the Asia Pacific regions. Eddie has a precise business perspective with substantial key strengths as a well-rounded leader. Managing a strong and dedicated sales and operations team across key markets, he provides consistent guidance and support in day-to-day operations. Eddie takes the seat in giving Security Solutions Today a bright-eyed spectrum of the organisation itself, what is in store for them in both the regional and global markets and future trends of the retail security industry.

Checkpoint Systems holds a notable reputation in its field. Keeping up with the constantly evolving retail industry has been one of the organisation's topmost priorities. For example, in this modern millennium, the popularity of Bring-Your-Own-Devices are intensifying amongst everyday people and pairing that up with wireless connections offered everywhere these days, this will have an impact on the retail industry. Eddie proceeded to rationalise that this change leaves a positive effect on Checkpoint, "I would say that this is more of a good thing than a bad one. Here at Checkpoint, we develop systems that android or iOS based. Even now restaurants are using iPads for customers to place their order. Everyone is moving towards the same direction and it is no different from us.

Eddie continues, "This is why we have our Merchandise Visibility solutions, which is geared towards to ensuring the safety and security of omni-channelling usage by consumers. With this high level of inventory visibility one can easily allocate the stock when the customer places an order online and reduces your working capital in the sense that you can have the right stock in its rightful place for the right customers."

As the technological world moves toward more and more advanced paths everyday, it becomes a highly anticipated question of how does existing technologies like Radio Frequency Identification (RFID) keep up. Rationalising its validity, Eddie says, "There will definitely be room for technologies like RFID in the future. This is the era where retailers will need to know exactly where their stock is at, and how many of that particular merchandise you have. It is because retailers will always need this kind of information to run a business smoothly and securely, that its legitimacy will never be lost."

The Asia Pacific region is quickly becoming one of the most niche hubs for retailers from all over the world. Different regions have different potential demands but for Checkpoint, many of their customers are international retailers and originated from Europe and from the US regions. In this aspect, the demands for retail security technologies, systems and products all regions are very similar. Most importantly Checkpoint ensures that they provide the same level of service for all their customers from the ASEAN regions, US regions and the Europe regions.

Checkpoint Systems caters to a variety of markets for example like departmental stores, grocery stores and even online shopping stores. Every vertical has its individual requirements and the value of the merchandises for each of the verticals different. Hence Checkpoint has different solutions fitted for various markets. When asked about the potential growing demand of the markets, Eddie replied, "Growth very much depends on individual country. If you take Vietnam for example, their supermarket/grocery vertical is growing rapidly – the rate at which this vertical grows is at ten newly opened stores within a span 3 months. Vietnam also has a projection of how many stores to be opened in 2 years time. So it really depends what the country is trending in at each particular period."

"But developed countries like Singapore or even Thailand; you can see a trend of the growth slowing down. This is why Checkpoint Systems is working hard at new inventive and innovative ways to help our existing customer database in increasing their Return of Investment (ROI) and prevent upcoming threats to their businesses. Our focus is not meant only for new or soon-to-be-opened stores, we are also looking into ways to help find better solutions for existing customers and their retail stores," Eddie continues.

Globally, we are modernising at a quick and comprehensive pace, as each retailer wanting to make every circumstance of retail be more convenient to consumers. Everything can be viewed online, in the comfort of one's own home and can

be purchased at a touch of a button. However Eddie predicts that even in 5 to 7 years time, there will always be a need for physical stores. He justifies, "Stores selling products like Apple – consumers will still want to come down to see, touch and feel the product and only then make decisions to purchase based on what they are looking at and holding onto."

Checkpoint Systems has a good and stable ground established in the industry. They have good partnering relationships with their customers and have been working with most of them for as long as 15 to 20 years. Expansion of the organisation in the APAC region is just one of its priority at present moment. Given its current position, Checkpoint Systems is ready to conquer the world of the retail security.

Checkpoint Systems' Customer Testimonial by David Lesmana, Director of Risk Management Redmart Limited (Online Groceries Store) in 2014

Having developed a working partnership with Checkpoint Systems for more than a decade or so, David Lesmana vouches for the organisation's professionalism and tenacity in providing the best-fitted solutions for their customers.

The partnership began when David decided to invest in Checkpoint's EAS system for their stores. David explains, "Before we started working with Checkpoint, we used a huge number of security guards just to help maintain the safety and security in our stores. But when they presented to us the EAS system and what it could offer, we just knew that benefits of the solution would be in a long-term basis. It helped reduced our overhead cost in the operations aspect whilst helping to deter criminal activities."

"Of course naturally, we were set to look for other alternative solution providers however after comparisons, we realised that we have yet to meet another with such comprehensive solutions and prompt after sales service support like Checkpoint's thus far", David validated.

There are many aspects to consider when choosing the most suitable solution provider. To David, speaking from his own experience, "The most important of all is to understand if the solutions fit the issues you are facing and if solutions are sustainable. Moreover, the price of the solution must be aligned to the organisation's yearly budget. Everything else like delivery, service and quality must be able to fit into these two considerations."

The retail world is one of the fastest evolving industries in the world. Looking back on his journey before and after partnering with Checkpoint, it has changed his perspectives on merchandising solutions, "In previous eras, when technology was not so advanced yet, we heavily depend on people/manpower. However, with the solutions – both physical products and systems – provide by Checkpoint, it has truly enhanced our productivity rate and efficiency to the business itself. They have given us convenience in running a systematically secured business," David pointed out.

When questioned about the three biggest benefits of working with Checkpoint Systems, David analysed, "Firstly, Checkpoint has a renowned reputation in the market – they have an impressive portfolio attached to them. They are able to provide a timely and responsive customer support, which is a very important and significant aspect to the loss prevention team in the field. To add on, they are always ever ready to help when a hiccup occurs in the system and is consistent in their availability of spare parts and technical support. Lastly, they have a team of experts who knows exactly how to cater to one's problems and needs holistically."

"Personally, I feel fully satisfied with Checkpoint's services and quality of solutions. I would definitely recommend Checkpoint to any organisation or anyone who needs a solution provider in the industry. They have an incredible sales support and has proven that they are one of the best in what they do", concluded David.

For more information, please visit: www.checkpointsystems.com SST

NEW MOBILE SURVEILLANCE CAMERAS ENSURES BEST FIRST RESPONSE

Article by Imran Aziz - Global Accounts Director, Xtralis, Matthew Naylor - Senior Product Line Manager for Video Analytics, Xtralis and Nicholas Dynon - Journalist

Surveillance has perhaps been the most significant legacy of 9/11. The continuing threat posed by global terrorism has driven huge amounts of government investment into electronic surveillance, as well as both wide and targeted physical monitoring systems in our cities. Digitised mobile camera surveillance in particular presents a powerful weapon in counter terrorism and law enforcement, yet this emerging technology remains relatively undiscovered.

The UK boasts one of the world's most extensive CCTV coverage. It is estimated that most individuals are seen by a camera an average of 340 times per day, and in Central London an individual will be on camera for about 95 per cent of the time. But compared to the UK, CCTV use in other jurisdictions is limited by a range of fiscal, legislative and privacy constraints. Surveillance cameras cannot be everywhere, and thus despite their ubiquity in modern streetscapes they lack the type of panoptic ability decried by civil libertarians.

Thus, even if a camera is effective in identifying crime within its own field of view, in all likelihood it has achieved this merely by shifting the crime to a location beyond the width of its lens.

According to the Queen's University Surveillance Studies Centre, the likely consequence of camera surveillance is that "crime and undesirable conduct are displaced into neighbouring areas once cameras are installed in a target location." The centre cited a San Francisco study, which found violent crime decreased within 250 metres of 'open-street' surveillance cameras, but increased beyond 250 metres. Crime, like water, finds the gaps and exploits them.

Filling those gaps is critical, and the introduction and use of new mobile camera technology has been heralded as the solution.

Mobile and born worn cameras

Mobile and body worn cameras have been traditionally used for the same purposes as static CCTV: deterrence and evidence. But it has been issues around use of force, such the 2014 shooting of Michael Brown in the St Louis

suburb of Ferguson, and the need to protect both police and civilians that have intensified calls for police to be wearing Body Worn Vest Technology (BWV). It has been recognised that the behaviour of both parties changes when a BWV system is involved.

The first empirical study on the use of body cameras by police was released last December by researchers at Cambridge University's Institute of Criminology. The results from this twelve month study of California's Rialto Police Department indicate a 59 per cent drop in use-of-force by officers wearing BWV and an 87 per cent drop in complaints against officers. These findings are consistent with those of similar studies.

Moreover, quite simply, if police and security personnel were not recording their actions in responding to an incident, then an onlooker with a smart phone/device would undoubtedly be recording their actions. According to the US Office of Community Oriented Policing Services, "given that police now operate in a world in which anyone with a phone camera can record video footage of a police encounter, body-worn cameras help police departments ensure events are also captured from an officer's perspective."

Echoing international trends, all

Australian state jurisdictions have now run trials of body cameras, but the approach has been one of caution.

"Whether we decide to roll body worn cameras out more widely across the organisation is not a decision we are going to rush", commented Inspector Ian Geddes of Victoria Police. "Further work is needed to help us to consider the next steps", he stated, "including considering the outcomes of other body worn camera trials happening across Australia and the world, as well as the on-going considerations around evolving technology and data storage needs."

Indeed, it is the evolving technology that is making law enforcement and security procurement of body worn cameras increasingly complex. While many organisations have trialled and implemented solutions based on transparency, evidentiary and behavioural benefits, emerging second-generation technologies are enabling cameras to do much, much more. The major consideration is now around whether to invest in cameras that can also provide live video feeds, immediate remote response and intelligent analytics aimed at early warning and intervention.

Gaps in first response

Traditional static CCTV and remote monitoring systems have been limited in providing first responders with real time information when responding to suspicious and or intercepting crime in progress. The majority of video surveillance systems are reactive in nature, in that they record the pictures delivered by video cameras on streets, which are later analysed for evidence or explaining crimes and other incidences. CCTV has been very effective, for example, in the hunt for Boston Marathon bombing suspects, but was of no value in preventing the incident.

Even when remote monitoring systems send alarms in real time to security monitoring centres, they are often poor in quality and require the attendance of a security response vehicle to investigate. According to Luke Percy-Dove of Matryx Consulting, "A very high percentage (95 per cent) of all alarm traffic is associated with false alarms, meaning most alarm attendances are a waste of time too." Typically Police will not attend an alarm event unless it can be validated or the premise carries a high level of priority.

Digital, or 'second generation' technology incorporating video analytics can turn existing technology into a proactive system. This allows alarm-receiving centres to make decisions with real time information, in many cases removing the need for security officer call-out. This results in a significant reduction in costs and false alarms, leading to improved security and proactive responses to situations as they occur.

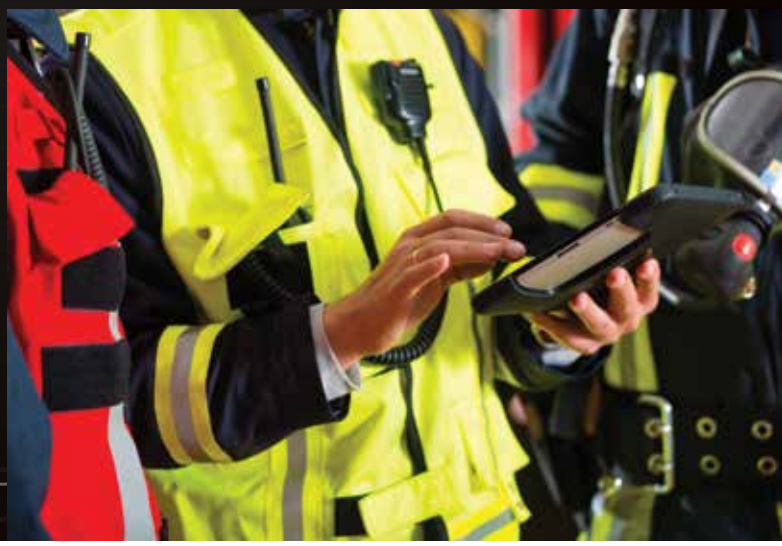
Once a first responder is deployed to an incident site, however, they still depend on radios to relay information back to central monitoring stations. In most jurisdictions this includes police, who are unlikely to have anything other than radio with which to communicate while on foot. According to Percy-Dove, this means that whoever is in charge of coordinating the response needs to rely on words to understand the situation on the ground. "In this day and age and with the technology available", he states, "it's crazy it still happens this way but people don't know better and what is possible."

Some first responders have the option of sending images from a car or transmission hub to the control, but this is limited by the necessity of being in close proximity to the hub. "As we all know, when a police officer is dealing with a situation they are not necessarily near or anywhere close to a car or hub", comments Imran Aziz of safety and security solutions provider Xtralis. "Also, these units will not be able to provide you with GPS information for use with mapping software."

Additionally, Percy-Dove notes, "some vehicles are now been fitted with video capability, but as far as I know these are recorded only in the vehicle and are not yet broadcast back to the station." In the case of the Victoria Police, Supt Geddes concedes that not all police vehicles are Mobile Data Network enabled.

First responder solutions

Body Worn Vest technology incorporating Personal Live Streaming Technology (PLST) can provide the potential answer to the real time intelligence deficit of radio only communications from first responder to base. "I think it adds real value because at street level you get to a whole different perspective of what has happened", states Percy Dovem "… the key is always to get the best possible information you can." However, it only works if it is plugged into a system that can transmit audio and video in real time to command and control structures so that the intelligence can be analysed and operational decisions can be made.



Entering the marketplace are a number of innovative solutions for early and reliable detection, remote visual monitoring for immediate and effective response. The City of London Police (CoLP), for example, has recently commenced a trial of an Xtralis solution that provides live transmissions from police vehicles and BWV to better assess situations and more efficiently deploy appropriate assistance.

According to Imran Aziz, the Xtralis HeiTel body worn solution has the ability to use multiple types of cameras with the same unit. The recording unit is remote from the camera, so if a member of the public pulls the camera off the vest, the recording remains safe on the vest, thus protecting the evidence. It also possesses a live streaming capability and GPS tracking. Xtralis' WCCTV Nano technology allows first responders to live stream wirelessly via 3G/4G, LTE and CDMA, as well as satellite, Wi-Fi and broadband networks. Its software allows multiple vests to be monitored at any given time, "giving the commanding officer complete situational awareness."
The HeiTel mobile technology is also used in other mobile applications such as public transport, cash in transit vehicles, and rental equipment and vehicles. "In principle the car unit will do everything the BWV will do but in addition it can have up to ten cameras on the unit, connect to panic buttons, blue light engagement, and audio systems to name a few", says Imran Aziz. "In Europe Xtralis developed a self-contained mobile early fire detection solution called RapidProtector, which utilises the HeiTel mobile technology combined with a compact area smoke detector to create a temporary mobile smoke detection solution for control rooms and base stations. It can be used during construction and upgrades when conventional fire panels need to be switched off."

In Australia local councils, water and electricity authorities are looking towards mobile video-streaming technology to protect assets and people in areas where there is no traditional network infrastructure available.

Water authorities are using the technology for use in pump stations or near dangerous drainage systems to proactively prevent unauthorised access. Used in combination with alarm sensors, a central monitoring station can be alerted when unauthorised persons enter a protected area, and an audio warning may be issued to the intruders in order to remove the threat.

Rob Galic, Sales Director at Xtralis says "Local councils are using the technology for Health & Safety to protect rangers who are driving in remote areas, and for protection of parking officers." According to Galic, tow truck companies whose drivers are often the target of aggression by vehicle owners

when their cars are being towed from illegally parked areas are also using it. "If the tow truck driver is feeling threatened or is concerned that their truck is at risk, they can hit a panic button that will alert a control centre and stream live video while recording the incident."

According to Wayne Trethowan of Hills Industries, when the system is paired with solar backup power units it provides a remote solution for builders and developers of broadacre estates who require video protection of assets and buildings before they become occupied.

Solutions such as these are making traditional mobile CCTV look archaic, and presenting law enforcement, public transport and security procurement departments with the choice between a deterrence and evidentiary tool on the one hand versus all that and a whole lot more on the other.

In essence, it is a choice between a tool that can record a criminal act and a tool that can proactively prevent one. Given the increasing political, social, financial and human cost of crime and the continuing spectre of terrorism, the latter option is difficult to ignore.

For more information, please visit: www.xtralis.com SST

Introduction

Martin Gren is co-founder and member of the Board in Axis Communications. As a well-respected industry pioneer, Gren led the team that developed and brought to market the world's first network camera in 1996. He has earned himself a PhD in entrepreneurship from Lund University of Technology in 2015 and was deemed as the world's most influential person in security by IFSEC Global in 2013. An impressive resumè attached to his name, Gren has made himself a well-renowned individual in the security world. Below is an interview with the man himself, giving us his latest insights about the Internet of Things (IoT).

AN INTERVIEW WITH

MARTIN GREN,
CO-FOUNDER OF AXIS COMMUNICATIONS AND MEMBER OF THE BOARD

The Internet of Things (IoT) has by far, taken over the world of physical security by storm, giving both solution providers and seekers an option to monitor and secure areas much more efficiently and conveniently. Can you explain why do you think that there is a definite need for the security world to embrace the IoT?

If you take a look at network cameras – they have always been embedded with IoT. Network cameras have their own web server and IP address, Ethernet plug and they have basically taken over half of the analog cameras. So now is the time that we will see more devices – for example the Network Horn Speaker launched by Axis Communications, embracing the IoT.

In a video surveillance system, when you put up a camera, the operator can see whoever that arouses suspicion. The operator will generally want a surveillance system that will allow him to explicitly warn the suspicious character that he or she is being watched. However, most video surveillance systems are not integrated like that.

An IoT device such as the Network Horn Speaker is pretty much self-sufficient in the way it can be addressed via the network and be configured – you can assign it to phone numbers so that you are able to just simply call it from your phone. The beauty of assigning a phone number to it is that it integrates with any system because you can just define a rule that if anything happens, you can just give that particular phone number a call.

In the security industry nowadays, we call it Internet of Security Things (IoST) because that is what it is for our industry. You also have other areas like Physical Access Control, which is also IP-enabled. Here at Axis Communications, we introduced an IP-based video door station, which is sort of an intercom and again using the benefits of IoT technology.

The IoT is indeed proving to be an

integral part of the security world as the years progress on. How has the IoT impacted the development of security technologies and what benefits will they be able to provide users over the current generation of surveillance that are already in use?

The important thing is compatibility and open standards, so that the whole system works together and can be expanded in scale but also by adding new device types covering new aspects. You can plan a platform that is centralised or de-centralised. The IoT technology really gives you all options and the rest is up to the organisation's standards and procedures to configure it in a certain manner. That is really the key benefit of having the IoST.

The IoST gives you foundation to congregate all the devices (e.g. surveillance cameras, physical access control etc.) to work together on one common system to ensure the safety of all the areas one would like to be monitored. It gives users a sense of convenience to get all the security devices to be controlled from one network.

As with many circumstances, there are mainly two sides to everything and while the IoT has certainly provided expediency and ease to the world of physical security, how does one ensure that physical security devices connected to the Internet, are protected from hackers?

You can typically put them on a local area network and you only have like a VPN tunnel into it from the real Internet. Although, technology is the same as the Internet, in reality however, you never connect these devices on the Internet, and quite frankly, it will be way too many devices. So you really need a piece of software that manages all the devices and it is that software that controls them. If the network is properly configured, it should be on a private network. This will reduce the possibility of hackers breaking into an organisation's IoST network systems.

The key here is to ensure that the piece of software used to manage all the devices is placed on a secured and private network where only authorised individuals are allowed to gain access to it.

According to Business Solutions, the "IoT will require physical security manufacturers and developers to work together in establishing baseline standards that allow physical security systems to work with devices beyond the confines of our industry." With all these steps in tow to setting up the IoT and physical security platforms, will this then incur more manpower cost for security solution seekers?

It will be just the opposite. It will help reduce costs. We have all the technologies now enabling us to implement a system for both centralised and de-centralised uses. It will require lesser manpower to operate the entire system as it can run from one platform and network. Instead of having different individuals monitor different security devices and respective systems separately, it can all be run and operated on one platform where it requires only one person to do so.

In that sense, the IoST really helps solution seekers by having to plan for less staff that is tied up to handle their organisation's security affairs. Embracing the IoST will definitely help in actually reducing cost.

The physical security world is an ever-changing game, consistently developing alongside technological advances. How does the IoT ensure that security is more safeguarded?

If you are talking about making security more safeguarded, traditionally, even a cable-enabled security device can be hacked just as easily. Take for example the Network Horn Speaker, if it was running on analog technology you would have no feedback because you would not know if it is actually working. However with a Network Horn Speaker, you have two-way communication via the network cable

so you can actually see that it is currently working or not. Additionally it has a microphone, so you can talk two-way. With network-based devices, you get higher reliability. Very often, a forgotten part of a video surveillance system is the maintenance – the very basic fact that you need to clean the camera.

According to Christian Brynes, the managing vice president at Gartner Inc., the AIC Triad model, which consists of three critical points for security – confidentiality, availability and integrity – will see shifts because of IoT. Byrnes said, "We're pretty sure that one thing that is happening is a push towards more transparency." Is this going to be one of the main challenges with IoT being on the rise? Do you think organisations will be comfortable in being transparent with their data information to a very large extent?

From an organisation point of view, I do not think it will make much of a difference. This will impact more on the security departments but they can set up various levels of access in a manner where they are not restricted by the technology, which has been the case in the past. When you have an analog speaker system, the only place is really where the microphone was. You could not do it remotely. Now with IoT technology, you are able to speak from the other end of the world even. I will be able to address my speaker from home and it can be played here.

Integrity and confidentiality is very much dependent on how you configure the system. Every system can either be well configured or badly configured and that is where the deciding factor lies. An analog system for example, if you have the microphone in a locked room, yes it was confidential but was not very much available.

There must be differences in the way security is managed and handled in heavily modernised countries and countries that are still far behind in their technological advancements. Does it make a difference, when in comparison to developed countries and developing countries, in the way and rate that they embrace IoT?

It very much depends on the solution seeker and how he perceives his security management of situations. An individual can come from a country not as modernised or technologically advanced but if presented with the best options by security solution providers, it is highly likely then that he will be willing to take up the offer of purchasing the best security systems or technologies there are in the market currently. Basically it all centres on the needs and wants of the security solution seeker. Different organisations embrace it differently.

What is your opinion on the upcoming network camera trends in Singapore?

In Singapore, we have slowly seen the market migrate from analog to Internet Protocol (IP) and now all new installations are basically done with full High Definition (HD) resolution. We see the multi-imaging cameras coming out, which are cameras in various different directions. We have seen the need for more light-sensitive cameras so that they actually can work during night time environmental conditions.

Maintenance will be a very important area because cameras can automatically tell that there are various failures somewhere in the system. I think, as a generic principle, the security managers should have better procedures for what to do when a camera fails and does not deliver proper images or videos. Both outdoor and indoor cameras in dusty environments should be cleaned at least once a year.

For more information, please visit:
www.axis.com SST

Attacks On Points Of Sales Systems

– A Special Report By Symantec

Article by Sanjay Rohatgi,
Senior Vice-President, Asia Pacific and Japan, Symantec

Background

The term POS (Point of Sale) device most commonly refers to the in-store systems where customers pay merchants for goods or services. While many POS transactions are in the form of cash, many of these payments are made by customers swiping their cards through a card reader. These card readers may be standalone devices but modern POS systems, particularly those in larger retailers, are all-in-one systems which can handle a variety of customer transactions such as sales, returns, gift cards and promotions. Most importantly from a security standpoint, they can handle multiple payment types.

Given the sensitive financial and sometimes, personal data to which modern POS systems have access, it is an obvious but not always well recognised fact that the security of these systems is of utmost importance.

POS security issues

Many all-in-one POS systems are based on general-purpose operating systems such as Windows Embedded, Windows XP and later versions, and Unix operating systems including Linux. Consequently, these systems are susceptible to a wide variety of attack scenarios, which could lead to large-scale data breaches.

Accessibility

All organisations that handle payment card data are required to implement safeguards set down in the Payment Card Industry (PCI) Data Security Standard (DSS). These standards help organisations to ensure that their systems and procedures are properly secured. The standard describes a concept known as the cardholder data environment (CDE) and the need to protect it. This is defined as "The people, processes and technology that store, process or transmit cardholder data or sensitive authentication data, including any connected system components."

The current standards recommend, but do not require the CDE to be network-segmented from other non-POS systems and the public Internet. While a strictly controlled and completely isolated POS system network would be quite secure, it is too impractical for serious consideration. The POS systems must be accessible for software updates and maintenance, allow business data to be exported to other systems (e.g. purchasing data and inventory), to export system and security logs, have access to required support systems such as network time protocol (NTP) servers (as required by PCI standards), and have connectivity to external payment processors.

Despite lacking a rule for segmentation, the PCI standards do mandate certain levels of access security, for example, if remote access from a public network is allowed, the access must employ two-factor authentication. In most mature retail environments, the CDE is appropriately segmented to reduce risk. However, in these environments pathways still exist from the general corporate network to the CDE.

While previous breaches have occurred by gaining direct access to POS systems, the most common attack route against POS systems is through the corporate network. Once an attacker gains access to the corporate network, for example through a vulnerable public facing server or spear-phishing email, the attacker could traverse the network until they gain access to an entry point to the POS network. This entry point is often the same, as a corporate administrator would utilise to maintain the POS systems.

Lack of point-to-point encryption (P2PE)

When an individual pays by swiping a card credit at a POS system, data contained in the card's magnetic stripe is read and then passed through a variety of systems and networks before reaching the retailer's payment processor. When this data is transmitted over a public network, the data must be protected using network level encryption (e.g. secure socket layer (SSL)).

However, within internal networks and systems, the credit card numbers are not required to be encrypted except when stored. Albert Gonzalez famously took advantage of this weakness in 2005 by infiltrating many retail networks and installing network-sniffing tools allowing him to collect over a hundred million credit card numbers as they passed through internal networks.

In response, many retailers today use network level encryption even within their internal networks. While that change protected the data as it travelled from one system to another, the credit card numbers are not encrypted in the systems themselves, and can still be found in plain text within the memory of the POS system and other computer systems responsible for processing or passing on the data. This weakness has led to the emergence of "RAM scraping" malware, which allows attackers to extract this data from memory while the data is being processed inside the terminal rather than when the data is travelling through the network.

Secure card readers (SCR) exist and have been implemented in some environments enabling P2PE, this can defeat RAM scraping attacks that work by searching the memory of the POS system for patterns of digits that matches those of payment card numbers. Such card readers encrypt the card data at time of swipe and the credit card number remains encrypted throughout the process even within the memory and underneath network level encryption.

Using P2PE within POS environments is not a new concept. Items such as PINs, when used with debit cards must be encrypted at the PIN pad terminal. When provisioning terminals, a payment processor or sponsor must provision the terminal by performing "key injection" where a unique encryption key is deployed directly to the device. With this scheme, the PIN remains encrypted at all times.

Software vulnerabilities

The majority of POS systems are running the older Windows XP version of Windows Embedded. This older version is more susceptible to vulnerabilities and therefore more open to attack. It should also be noted that support for Windows XP would end on April 8, 2014. In practice this means, no more patches will be issued for any software vulnerabilities found in the operating system from the cut-off date. This event will certainly place POS operators under increased risk of a successful attack and POS operators should already have mitigation plans in place to meet this coming deadline.

Susceptibility to malicious code

As many POS systems are running a version of Windows, they are also capable of running any malware that runs on Windows. This means that attackers do not need specialised skills in order to target POS systems and malware that were not specifically designed for use on POS systems could be easily repurposed for use against them.

Slow adoption of EMV

Europay, Mastercard and VISA (EMV) is a set of standards for card payments. It is often referred to as "Chip and PIN" and is a replacement for traditional magnetic stripe based cards. EMV cards contain embedded microprocessors that provide strong transaction security features. EMV never transmits the credit card data in the clear mitigating many common POS attacks. EMV cards are also less attractive to attackers as they are difficult to clone.

While EMV is commonly used in some parts of the world such as Europe, US merchants in particular have been slow to adopt the EMV standard and will not start implementing it until 2015.

Typical anatomy of attacks against POS systems

Attacks against POS systems in mature environments are typically multi-staged. First, the attacker must gain access to the victim's network. Usually, they gain access to an associated network and not directly to the CDE. They must then traverse the network, ultimately gaining access to the POS systems. Next, they will install malware in order to steal data from the compromised systems. As the POS system is unlikely to have external network access, the stolen data is then typically sent to an internal staging server and ultimately exfiltrated from the retailer's network to the attacker.

Infiltration

There are a variety of methods an attacker can use to gain access to a corporate network. They can look for weaknesses in external facing system, such as using an SQL injection on a Web server or finding a periphery device that still uses the default manufacturer password. Alternatively they can attack from within by sending a spear-phishing email to an individual within the organisation. The spear-phishing email could contain a malicious attachment or a link to a website which installs a back door program onto the victim's machine.

Network traversal

Once inside the network, the attackers need to gain access to their ultimate targets – the POS systems. Attackers will typically use a variety of tools to map out the network in order to locate systems within the CDE. While they may use vulnerabilities or other techniques to gain access to these systems, often the simplest, yet effective method of gaining access is by obtaining user credentials. User credentials may be obtained through key-logging Trojans, password hash extraction, cracking, and/or replaying captured login sequences, or even brute force.

Eventually, administrative level credentials may be obtained. Attackers may even gain control of a domain controller, giving them full access to all computers in the network. Once in control, they can then gain access to the CDE even if it is in a segmented network by using network and data pathways established for existing business purposes. Once inside the CDE, they then install malware, which allows them to steal card data from the POS systems.

Data-stealing tools

Malware, which is purposely built to steal data from POS systems, is widely available in the underground marketplace. In some attacks, network-sniffing tools are used to collect credit card numbers as they traversed internal unencrypted networks. Other times, RAM scraping malware is used to collect credit numbers as they are read into computer memory. Any collected data is then stored in a file locally until time for exfiltration. Often, this data file needs to be transferred to multiple computers hopping through the internal network until reaching a system that has access to external systems.

Persistence and stealth

Because the attacker is targeting a POS system and these attacks take time to gather data, they will need their code to remain persistent. Unlike database breaches where millions of records are accessible immediately, POS system breaches require the attacker to wait until transactions happen and then collect the data in real-time as each credit card is used. Because of this, early discovery of the attack can limit the extent of the damage. Malware persistence can be achieved using simple techniques to ensure the malware process is always running and restarts on any system restart.

Stealth techniques used will vary from simplistic obfuscation of filenames and processes to specific security software bypass techniques. In more secure environments, in order for attackers to succeed, they will likely already have access to compromised administrative credentials and can use them to scrub logs, disable monitoring software and systems, and even modify security software configuration (e.g. change file signing requirements or modify whitelisting entries) to avoid detection.

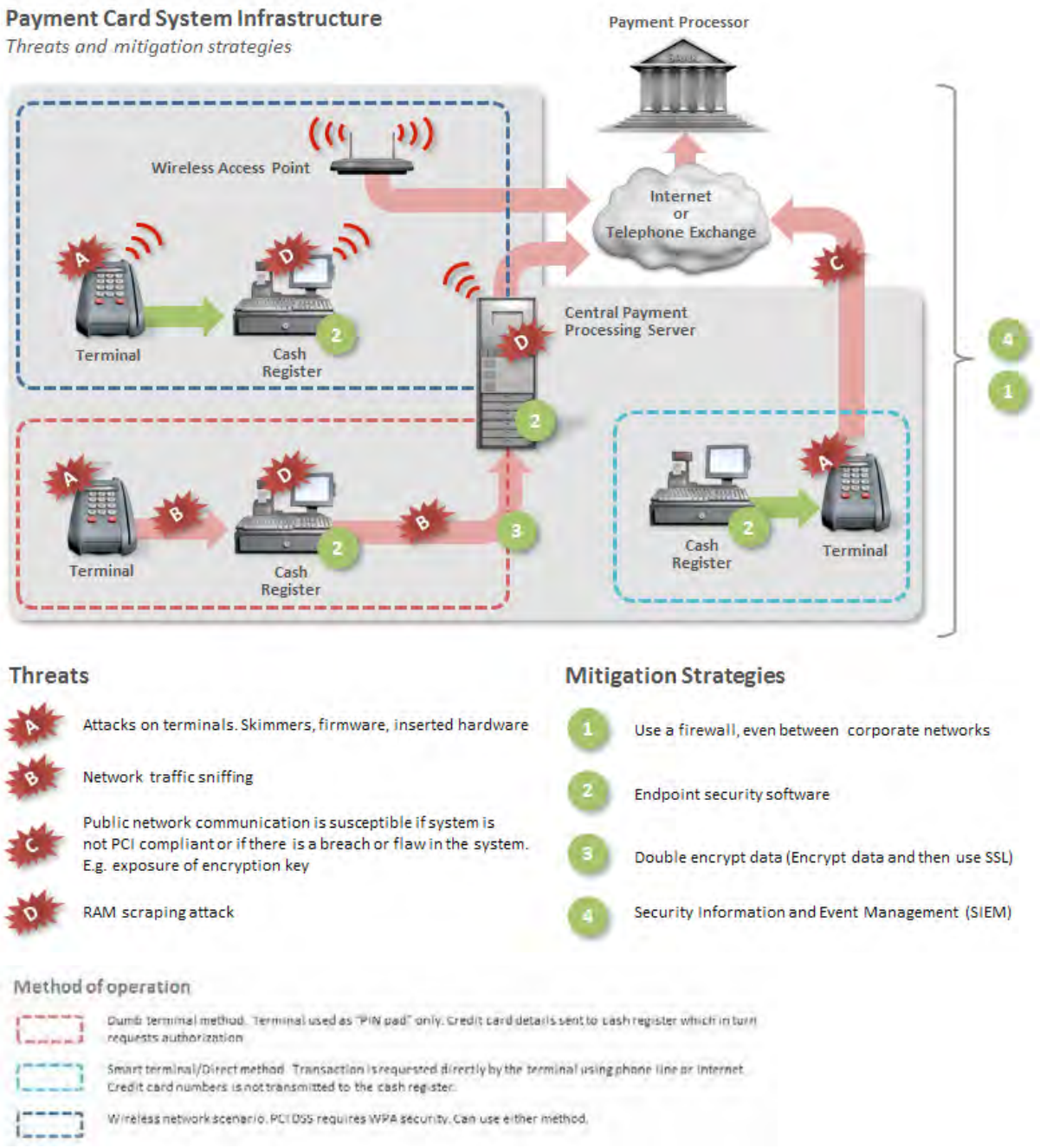


Figure 1: Threat to payment card system and possible mitigation strategies

Exfiltration

The attackers may hijack an internal system to act as their staging server. They will attempt to identify a server that regularly communicates with the POS systems and piggyback on normal communications to avoid detection. Any data collected by the RAM-scraping malware will be sent to this staging server where it stored and aggregated until a suitable time to transmit to the attacker. At the appropriate time, the attackers may transfer the collected data through any number of other internal systems before finally arriving at an external system such as a compromised FTP server belonging to a third party. By using compromised servers from legitimate sites to receive the stolen data, the traffic to these sites are less likely to arouse suspicion on the part of the compromised retailer, particularly if they are sites that are often visited by users within the victim organisation.

Protecting POS systems from attack

There are many steps that POS operators can take to reduce the risk from attacks against POS systems. The following diagram illustrates the typical infrastructure of payment card systems and the threats against them along with mitigation strategies that can be employed at various points in the system.

Practical steps to take

- **Implementation of PCI Security Standards**

  - Install and maintain a firewall to facilitate network segmentation
  - Change default system passwords and other security parameters
  - Encrypt transmission of cardholder data across open, public networks
  - Encrypt stored primary account number (PAN) and do not store sensitive authentication data • Use and regularly update security software
  - Use intrusion protection system (IPS) at critical points and the perimeter of the CDE
  - Use file integrity and monitoring software
  - Use strong authentication including two-factor authentication for remote systems
  - Monitor all network and data access (SIEM)

- Test security systems, perform pen-testing, and implement a vulnerability management program
- Maintain security policies and implement regular training for all personnel
- Implement multi-layered protections including outside the CDE. Typically, the attacker will need traverse multiple networks and layers of security before reaching a POS system. Any single layer that the attacker is unable to bypass prevents successful data exfiltration.
- Implement P2PE or EMV ("Chip and PIN")
- Increase network segmentation and reduce pathways between the CDE and other networks
- Maintain strict auditing on connections to between the CDE and other networks. Reduce the number of personnel who have access to systems that have access to both the CDE and other networks.
- Employ two-factor authentication at all entry points to the CDE and for any personnel with access rights to the CDE
- Employ two-factor authentication for all system configuration changes within the CDE environment
- Implement system integrity and monitoring software to leverage features such as system lockdown, application control, or white-listing

For more information, please visit: www.symantec.com SST

Dahua Provides IP Solution For Sucre's Safer Tomorrow

Introduction

Dahua Technology successfully helps to secure Sucre, the constitutional Capital City of Bolivia. Sucre, historically known as Charcas, La Plata and Chuquisaca is located in the south-central part of the country. With a population of 247, 300, the city is listed as the 6th most populated in Bolivia and is divided into eight districts, including five urban and three rural districts, including five urban and three rural districts.

Challenge

Sucre, as a developing city is facing many problems such as traffic flow issues and crime. The municipal government is determined to create a better and safer living environment for its citizens by launching safe city project with an urban surveillance deployment project.

Solution

Dahua, together with a local distributor, Digital Security System SRL, enable Sucre to meet its goals of a better and safer city by offering a customised urban surveillance solution. This solution includes Network PTZ cameras (SD6A230N-HNI and SD59230S-HN) that are installed in different zones of the city, connected by wired and wireless IP communication.

Between the two models mentioned, SD6A230N-HNI becomes the main product adopted. With powerful 30x optical zoom, triple-stream encoding support, and up to 60fps@720P and 30fps@1080P resolution, the devices perfectly meet the high standard requirements of the project. As for the outdoor surveillance functions, this series also proves itself capable with an IR distance up to 150 metres and featuring great day/night performance in any lighting conditions.

The central control centre features Dahua's Digital Surveillance System 7106D, their first embedded general surveillance management console which integrates software and hardware together. In the control centre, all the video can be stored for 30 days to fit the customer's requirement.

"We appreciate having Dahua, a responsible and professional company, as our partner," said Harold Ribera, Line Manager at DSS SRL. "The clients were unfamiliar with the new system at first, but Dahua's team of expertise help solve the bugs and problems with effectiveness."

Conclusion

"It is an honour for Dahua to be able to take part in the safe city project in Sucre," said William Zhou, Sales Director of Latin-America at Dahua Technology. "The results are obvious. After only a few months in operation, the whole area has seen a decrease in vandalism, theft, and violence. Dahua uses its advanced IP solution to secure property and people in Sucre. The long-time rigorous support from Dahua is highly regarded by the clients. We will continue to offer our strongest support and service."

For more information, please visit: www.dahuasecurity.com SST

Digital Billboard Company Innovates with Axis and Milestone Integrated Video and IBM Audience Analytics

Challenge

When it needed a targeted campaign to attract the attention of potential buyers on their way to the Melbourne airport, Porsche worked with billboard supplier oOh! Media, the largest audience-reaching digital advertising network in Australia. It has a diverse product offering across road, retail, airport, café, venue, study, social sports and experiential opportunities throughout Australia and in New Zealand.

Porsche wanted to take advantage of the flexibility and creativity that digital billboards provide. The challenge to oOh! was to create a smart billboard that was able

to detect Porsche vehicles and display a custom message to their existing customers. To accomplish this, oOh! searched for technology that was capable of analyzing all oncoming vehicles to identify potential customers, and fast enough that they could display targeted content to those vehicles in seconds.

Solution

Melbourne marketing technology firm Intelliscape was hired to create the billboards. John McGiffin, Managing Director at Intelliscape, designed the solution, which included Axis Q1615E network cameras mounted on the billboard. The cameras feed into Milestone XProtect Essential video management software (VMS) whose open platform enables interoperability with other systems. McGiffin's solution integrates the VMS with his proprietary tool for car recognition that can pattern-match the vehicles against a database of known cars. McGiffin also employed IBM video analytics, forming a powerful, tailored solution.

Advantages

The custom-integrated solution immediately recognises the targeted audience and delivers custom billboard advertisements accordingly. The Axis cameras provide

high-resolution shots of the cars, and the feeds can be viewed and shared easily with the Milestone software. Milestone is able to manage different streams and resolutions without delays or technical difficulties.

Benefits of open platform architecture

McGiffin is currently using Axis cameras on the billboard, but appreciates the flexibility that Milestone's open platform affords. The software supports over 150 different brands of network video cameras in thousands of models.

"This is the first pilot project with oOh! Media, but this security solution is portable," McGiffin says. "I like the idea that I can choose any camera vendor for other projects based on cost and functionality and be confident that integration will go smoothly. It's a great thing not to have to worry about."

Ease of use impresses partner and customer

McGiffin is no stranger to traffic monitoring. He designed a system that used IBM video analytics to monitor people in supermarkets, specifically focusing on customer traffic at certain times of day as well as people's age and gender.

"I first heard about Milestone through IBM," McGiffin says. "They did all of their testing with Milestone. When I started looking into it, I saw how powerful a platform it is. I also found it to be really intuitive and easy to use."

John Purcell, Commercial Director at oOh! Media, says he was also impressed with Milestone's video management capabilities.

"When John first showed us the VMS, I was amazed the possibilities," Purcell says. "It is easy for us to both look at our audience and provide quantitative data to our advertisers."

Looking to a smarter future

Purcell and McGiffin both see this project as the beginning of an exciting new trend.

"There's lots of interest in how to make billboards smarter," Purcell says. "With technology such as this providing us the ability to monitor and analyse traffic, we are looking at how this could create amazing new opportunities for our advertisers to connect to our audiences."

Purcell says that European companies have already expressed interest in purchasing the proprietary solution, and Porsche has been so pleased with the campaign that discussions about expanding the solution worldwide are under way.

"I've been swamped with offers to purchase the solution John has created," Purcell says. "It's an exciting time for digital advertising. There is a lot of potential to push it further, and Milestone video technology is right at the heart of it all."

For more information, please visit: www.milestonesys.com or www.oohmedia.com.au SST

Dahua IP Solution Secures Arezzo In Italy

Introduction

Dahua Technology together with Videotrend, provided an effective video surveillance monitoring system to secure the city of Arezzo to meet the city administration high security standard requirements.

Arezzo is a city in Italy, capital of province with the same name, located in Tuscany. Arezzo is known for its churches, museums, fabulously sloping Plazza Grande, and gold item production.

Solution

Dahua's specialists delivered a high innovative and reliable IP solution for to ensure the safety of the city. Their network camera feature a 2-Megapixel progressive scan Exmor CMOS sensor, providing high quality images at 25/30fps @1080p. It supports H.264 and MJPEG dual codec and smart detection. With 30 metres IR range, the camera performs well in all lighting conditions, day and night.

ITC series cameras with a highly efficient algorithm provide intelligent surveillance for roads, streets and venues to monitor traffic conditions. With its HD image resolution function and the speed shutter at 1/25 - 1/100000, these devices can capture ultra-clear images of vehicles and recognise license plates, even when they drive at a very fast speed. These intelligent devices have integrated Optical Character Recognition (OCR) and can be used for Red Light Enforcement.

Dahua Super NVR6000DR series with up to 128-channel capacity and front LCD display were used. This model has redundant power supply modules and also supports multi-brand network cameras, including Arecont Vision, AXIS, Bosch, Brickcom, Canon, CP Plus, Dynacolor, Honeywell, Panasonic and more. With its support for RAID0/1/5/6/10/50/60, data protection can reach maximum safety and reliability.

Conclusion

"Dahua offers intelligent security solutions that enables a smarter and safer Arezzo," said Elmer Zhang, Sales Director of Europe at Dahua Technology. "The excellent qualities of the images obtained even in extreme light conditions enable uninterrupted monitoring of areas at risk, and therefore Dahua has realised its goal of protection for local residents and tourists in Arezzo."

For more information, please visit: www.dahuasecurity.com/ SST

Galaxy Control Systems Protects Patients And Staff At Psychiatric Hospital

Introduction

Highland-Clarksburg Hospital is a 150-bed behavioral psychiatric center located in Clarksburg, WV. Its patients include forensics patients (deemed unfit to stand trial and/or non restorable), dual-diagnosis substance abuse patients, children and adolescents and intellectually challenged individuals.

In August 2013, the center officially opened its $23 million renovation of a 415,000-square-foot former critical care hospital building, donated in 2010 by United Hospital Center after it moved to a new facility. When renovation commenced in January 2013, the project was fast-tracked.

The Security Office at Highland-Clarksburg Hospital allows staff to manage the access control and video surveillance at the facility.

Challenge

The renovation required a number of structural upgrades, such as impact-resistant drywall, secure lighting and other fixtures, plus a state-of-the-art security system to protect the hospital's patients and staff as well as the surrounding community. The scope of the security installation included access control, patient tracking, overhead paging, fire alarm upgrades and HD video surveillance systems.

"The initial push on this project was to protect the patients from the outside and the outside from the patients. It is very high-security, and we have all the bases covered," says Renay Jarrell, President of systems integration firm Appalachian Signals and Products Inc. (ASAP) of Winfield, WV. Renay and Randy Jarrell are co-owners of ASAP, the integration firm that was contracted to perform the security upgrades.

Mike Casdorph, Director of Facility Development for Highland-Clarksburg Hospital directed and oversaw construction for the project added, "The project was fast tracked as we wanted to get portions of the facility open and ready to accept patients. I cannot say enough about the Contractors and ASAP as they all went above and beyond to meet our schedules. I am very impressed with the Galaxy system and the installation and service provided by Renay and her team. They are always available to assist if we have a problem."

From the start, the project had the potential to cause major headaches along the way. In addition to the traditional challenges of securing a psychiatric centre – particularly one that houses forensic patients – the high profile of the project and the speed of construction posed a number of challenges for ASAP.

Solution

For the access control piece, ASAP chose Galaxy Control Systems proximity card systems. In all, ASAP has installed 208 readers, 24 power supplies and 20 Galaxy controllers throughout the facility. As with nearly any facility, ASAP was tasked with securing the exterior doors at

Highland-Clarksburg Hospital, but where this project differs from others is in the need to also secure interior doors to patient floors. This is an extremely crucial necessity given that three floors are used to house psychiatric patients.

The Galaxy system is supplemented by an additional layer of protection requiring users to input a five-digit PIN to identify who is accessing what areas of the facility and to ensure adherence to established hospital policies and procedures. All interior doors in the patient care areas are locked and can only be opened with the swipe of the badge and the inputting of the unique pin number by the staff. This double security means that if a badge is misplaced or stolen, it can't be used to move through the facility, as the person would still need the PIN. The system is also used for all of the elevators with a card swipe and pin required to call an elevator to a floor and once inside the elevator a card swipe and PIN is also required to move between floors.

"When you get to the higher-security areas, the Galaxy system teams up with the patient-tracking system to allow entrance to another door or an elevator," Jarrell says. "And because this is a hospital that still has some unoccupied areas, those areas also have the door mechanisms to lock unauthorised individuals out."

Aside from the logistical challenges posed by the facility's construction timeline, the biggest challenge ASAP faced was interfacing the access control system with elevators. The main problem was to allocate elevator cars to certain staff members at certain times of day – a challenge exacerbated by the fact that elevator manufacturers typically do not focus on physical security concerns. To overcome this obstacle, ASAP installed card readers strategically and took advantage of the integration between the access control and patient tracking systems to protect the card readers with stringent access control rights. If a hospital staff member is escorting a high-risk patient, elevator doors cannot be unlocked without setting off an alarm unless both the patient-tracking reader and access control badge are married.

Systems integration firm Appalachian Signals and Products Inc. (ASAP) of Winfield, WV were contracted to perform the security updates (from Left to Right Adam Jarrell, Renay Jarrell and Randy Jarrell).

When it came to sourcing access control readers, there was no competition between products, Jarrell says. ASAP has used Galaxy's systems since 2002, and has used the company's products exclusively for more than nine years. The high performance delivered by Galaxy systems, along with their low maintenance requirements, are the primary reasons ASAP has been loyal Galaxy customers for so long. "The IP protocols their readers use have worked out well, and we've had very few issues on-site to date," says Dennis Carney, lead integrator for ASAP. "The structure, the equipment and the ability to keep it running without a whole lot of hands-on work were the other reasons we chose Galaxy's products."

Conclusion

"For me, the fact they are a United States-owned company is very important. You can actually talk to tech support with ease, and they are very available to my techs in the field. In our industry it's a little unusual that you get to deal with somebody in the States with tech support and get that quick response. That means an awful lot," Jarrell says. "We're a small family business in West Virginia, and in West Virginia, your reputation means the world. So we truly try to keep our business in the USA as much as we possibly can, and Galaxy represents that to us. We've also had a good working relationship with them and have been impressed with their line for a lot of years."

For more information, please visit: http://www.galaxysys.com/ SST

EtherWAN Helped The PoE Connectivity In Hospital Surveillance In Taiwan

Introduction

The public health care system is important to metropolitan areas. A principal medical center in Taiwan houses advanced equipments, technologies and professional staffs and takes care of many incidents of emergency and major illness and injuries.

As the leading medical center, the hospital thrives to provide patients with the most secured medical environments. A reliable surveillance system upgrade is required by the hospital to monitor patients' conditions and to minimise medical disputes over the recordings.

Technology

Although there has been analog surveillance system installed in the hospital buildings, the client wants to install more cameras and to integrate the new surveillance system with the hospital network. Therefore, Ethernet technology is implemented because of scalability and availability.

Power over Ethernet (PoE) technology is utilised in both the network cameras and network switches. Complied with IEEE802.3af or IEEE802.3at standards, the PoE switches deliver both power and data over CAT.6 cables, up to 15.4 watts or 30 watts for each PoE camera. The monitoring will be achieved by NVR (Network Video Recorder) and VMS (Video Management System) installations for instant data reviewing and real-time video monitoring via LAN or Internet. A redundant network is required in order to prevent data loss and uninterrupted surveillance.

Challenges

There are three main buildings in this hospital, which previously installed separate analogue surveillance systems at each building. To begin the system migration, it requires Ethernet connectivity all across the surveillance

area. With the provided cabling, the network devices have to work in harmony with the whole surveillance system, as well as to form a redundant network topology.

For smooth and stable surveillance results, network redundancy and sufficient bandwidth are essential for uninterrupted data transmission. Also, in a case of maintenance, technicians prefer easy troubleshooting.

Solution

The client eventually plants fiber optic cables among the main buildings, in order to transmit data over hundreds of metres away.

The partnered system integrator selects EtherWAN's EX17082, EX17162 and EX17242 PoE switches, which provide 8, 16 and 24 PoE/PSE ports, respectively. They are utilized as power sourcing equipment (PSE) to power up the PoE network cameras. The NVRs are also connected to the switches for video footage storage. These web-smart switches allow users to reboot the devices or turn off/on PoE remotely via a web browser, saving hassles when it comes to camera setups.

In the main server room, EtherWAN's EX25611 managed Gigabit Ethernet switch is deployed to receive video recordings from the NVRs. The EX25611 features four 1G/10G SFP+ uplink ports, connecting to a Layer 3 core switch and the CMS server.

The installed EtherWAN Ethernet switches are all equipped with fiber optic uplink SFP slots to help forming network redundancy when demand calls for future upgrade.

Product selection

EX17242
Web-smart 24-port 10/100BASE-TX PoE and 2-port combo Gigabit SFP Ethernet Switch

EX17162
Web-smart 16-port 10/100BASE-TX PoE and 2-port combo Gigabit SFP Ethernet Switch

EX17082
Web-Smart 8-port 10/100BASE-TX PoE (IEEE802.3at) and 2-port combo Gigabit SFP Ethernet Switch

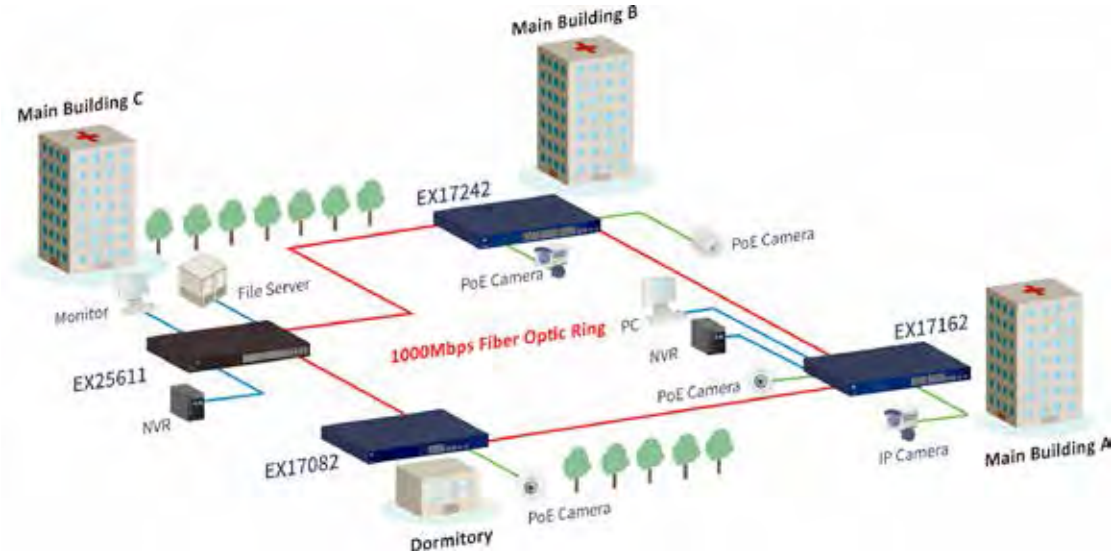
EX25611
Managed 24-port 10/100/1000BASE-T (4-port SFP Combo) and 4-port 1G/10G SFP+ Ethernet Switch

Results

Over 460 brand names of PoE cameras and NVRs are connected with 50 units of EtherWAN PoE switches on site, which are fully compatible with the camera vendor's VMS software, running altogether seamlessly. The security personnel are able to monitor the whole hospital and to review video evidence any time.

By utilising such digital surveillance network, it enhances the total safety of the hospital's patients, staff and assets. Furthermore, the high-resolution video records come in handy for medical dispute resolutions.

For more information, please visit:
http://us.etherwan.com/ SST



AN INTERVIEW WITH

MANAGING SANJAY AURORA, MANAGING DIRECTOR, ASIA PACIFIC, DARKTRACE

Cyber security threats often come from several different directions and its threats are constantly evolving, aligned to the changing trends of the cyber world. Does cyber threats in third world countries differ from those faced in first world countries like Singapore? Is there a need to take more radical measures?

I think it is not so much tied to whether it is a technologically advanced country or otherwise. The relevance today is that cyber threats are getting more and more unknown that is what Darktrace specialises and emphasises on, that the enterprise immune system, which sits on the network uses the complexity of your network to your strength. This is the reason why, as the threats evolve, Darktrace's approach makes it even stronger when it comes to protecting your network and your enterprise.

Between the evolving nature of economies or state of affairs, in my opinion everyone is vulnerable right now. The more sophisticated countries like Singapore and Australia poses a different kind of attractions to the bad actors. The undeveloped or developing IT security-orientated nations provide a different kind of opportunity to the bad actors.

So if you look at it, the bad actors use both these areas because either way, it is a win-win situation for them. The more mature you are, the more lucrative you get to them as an opportunity. That is why I think vulnerabilities exist equally and the need for a different thinking in cyber security, which Darktrace provides, is absolutely needed to counteract these potential hazards.

The human culture in this era is heavily dependent on BYOD gadgets like mobile phones and tablets and coupled with today's technologies, portals can be accessed from literally anywhere. How does this change or affect the preventive methods used for cyber threats?

This proves the fact that every organisation can no longer work on the terms of privacy because social media platforms are a main source of channel to promote anything and everything they need to promote. Organisations are past that era where the first thought comes to mind is to 'build a fence' or 'build a fortress'. So the very knowledge that people has to cross onto such platforms and retrieve information or details has just increased the level of cyber threats that will come in.

Threats will find its way in no matter what. The only difference is that the conventional way of thinking, which is 'Building the biggest wall around me will save me", will not work anymore. It is getting weaker and weaker. What you need to do is to think of how to map all these devices and form that pattern where you are spotting anomalous behaviours before it becomes damage. That actually is one of the triggers for technologies like Darktrace to get more and more relevant.

The Asia Pacific region spans across from countries like Thailand to Australia. According to analysts, the Cyber Security market in the APAC is expected to grow at a compound annual rate of 15 per cent over the period of 2014 - 2019. What are your thoughts on the growth of the cyber security market in the APAC region? Do you agree with this analysis?

I certainly agree, cyber security market is expected to

grow. The stakes are higher than ever before, the risks are higher and this market will need investment. The question is, which areas will need investments, which is about prevention and detection and we will believe a lot more growth will come in the area of early detection. Prevention is no longer working as effectively as before and because of this people will start investing more in early detection and on layered security.

Human and machine behaviours play an integral role in cyber security risks and threats. How integral are these roles in imposing limitations to the process of mitigating cyber threats and risks? What are methods or practices put out by Darktrace in observing human and machine anomalies that contributes to cyber threats and risks?

The threat actors will come in from the weakest link, they will find ways. Sometimes they will also leave the machine that got compromised for a couple of hours because they know that people will start looking for them soon. So that is the kind of behaviour that they demonstrate and if you look at our adaptive modelling of the network, our machine learning capability, what we do is we look for abnormal behaviours.

The bad actors are not able to perverse from the places, finding the right areas without disturbing the pattern of life. They know exactly what people are looking for and because of that they will stealth and not break any rules nor visible. However for these bas actors to replicate the network behaviour without showing some kind of abnormalities in the network is almost impossible.

As a prominent cyber security solution provider that covers worldwide tracks with its expertise, what are the kinds of challenges that Darktrace face? Are there any kind of limitations imposed due to a country's lack of technological infrastructure and means? If so, how does Darktrace plan on overcoming them?

Darktrace is relatively new in the cyber security market in APAC for example. Our challenge really is the education of customers – there are sophisticated customers and customers who has experience and who has in-depth knowledge in what obstacles they are facing in terms of cyber threats – however there are still some sectors or industries where need to learn more about cyber threats and security.

Darktrace was founded in 2013 by leading machine learning specialists and government intelligence experts and opened its APAC headquarters in Singapore. How does Darktrace intend on making a stronger presence in the APAC region? What are Darktrace's plans in tow for the next 5 – 10 years in Asia Pacific?

We have gone from one to 12 employees and by the end of the 2015, we should hit about 18 employees altogether. We are already present in Japan, New Zealand, Australia and Singapore. We are opening up in India and very soon in Hong Kong and Korea. Darktrace is on a rapid trajectory and by the time we reach 2016, I expect us to double the numbers in the APAC region.

For more information, please visit:
www.darktrace.com SST

WIDE DYNAMIC RANGE IMAGING

Article by Michael Korkin, PH.D. Vice President of Engineering

Introduction

By standard definition, dynamic range is a ratio between the largest and the smallest value of a variable quantity, such as light or sound. Difficulties in understanding and applying the dynamic range concept revolve around the question of its measurement.

Consider a task of measuring precipitation rate using a bucket. In a heavy rain downpour, the bucket would quickly overflow making it impossible to determine the largest value of precipitation: the results would be clipped at the bucket capacity level. In light rain, the bucket would sporadically receive a drop during one measurement interval and two during another, making the smallest value uncertain, or noisy. To increase the certainty of small value readings, a longer collection time is needed, but this does not work for the large values, it causes the overflow.

Needs Shorter Capture Time **Needs Longer Capture Time**

This basic example illustrate how measurement is in fact an information channel: it can convey, lose or distort information about the variable quantity, either at the top of the range, or at the bottom, or at both ends at the same time.

Consider a video camera as a measurement instrument. It measures the amount of light falling onto each its millions of light-sensitive elements, or pixels, arranged in a two-dimensional array. Each pixel integrates the photon flow it receives over a period of time, and then converts it into an electrical signal to be read out. If the photo flow arriving from the scene is strong, or if the integration time is long, the signal may hit the limit and saturate. Then, all luminosity variations that correspond to fine details of the bright areas of the scene will be lost. Similarly, if the photon flow from the scene is weak, or if the integration time is short, the signal will produce uncertain, noisy readings, and all details of the scene will be lost.

As in any information channel, the quality of the video camera can be judged by how well it conveys the information, that is the luminosity variations present in the scene. In particular, is the camera able to capture subtle variations in the highlights of the scene without clipping? Is it able to capture subtle variations in the shadows without drowning them in noise? What about capturing scene details at both ends of the dynamic range capability of the camera as a measurement instrument?

Generally, if the dynamic range of the scene is the same or narrower than that of the camera, the resultant images would faithfully convey scene details both in the shadows and in the highlights of the scene with no noise or clipping. If the dynamic range of the scene is wider, the camera would either clip details in the highlights, or mask details in the shadows by excessive noise, or do both at the same time.

How can the dynamic range of the scene be evaluated independently of the camera's own capability? This can be done piecewise by taking multiple scene captures at different exposure times. Very long exposures reveal details in the shadows while saturating the highlights. Very short exposures reveal details in the highlights while drowning the shadows in the noise floor. The ratio of the longest exposure time required to reveal details in the shadows to the shortest exposure time to reveal details in the highlights provides a reliable estimate of the dynamic range of the scene.

Why is dynamic range limited?

The dynamic range limitations come from multiple causes, primarily from the physical properties of the light-sensitive pixels of the image sensors. Consider two identical image sensors that are different only in the area size of their light-sensitive pixels, and their well capacity related to the size. Which sensor would have a wider dynamic range? The answer is: the one with the larger pixels. On top of the range where the light flow is very strong they will not saturate as readily as the smaller ones, due to larger well capacity. On the bottom of the range where few photons are present, the larger surface area of sensitive pixels will gather more photons and reduce the uncertainty (noise) of the small value readings.

A conflict between the need to increase the size of sensitive pixels for achieving a wider dynamic range, and the need to make them smaller to increase spatial resolution, is always present. Often, spatial resolution, which is nominally high due to small size of pixels, is seriously compromised by their narrow dynamic range, which causes either noise, or clipping, or both. Noise masks delicate signal variations containing fine image details in the shadow, while clipping erases the highlight details.

Contributing to the conflict between the dynamic range and the spatial resolution is the temporal aspect of imaging – objects in the field of view may be moving, causing motion blur. Motion blur is a reducer of spatial resolution because it smears the moving objects over multiple adjacent pixels. A need to reduce motion blur demands shorter integration time, but that, in turn, raises measurement noise. Noise also destroys spatial resolution by masking subtle signal variations. To summarise, the effective sensor resolution may be lower than the nominal due to narrow dynamic range of small pixels, due to motion blur, and due to measures intended to reduce motion blur.

It is the ratio, not the absolute range

An important attribute of the dynamic range concept is that it is defined as a ratio, and not as an absolute value. This means that different scenes with an identical dynamic range

may have entirely different average luminosity, or the absolute range. The same effect of shifting the range up or down is produced by the camera's aperture, which limits the amount of light reaching the image sensor. So, a camera specified to support a particular dynamic range will produce different results for different absolute ranges and different apertures because its own capabilities do have absolute limits, primarily due to physical size of its pixels. In particular, a scene with a given dynamic range but a lower average luminosity (or a smaller aperture) would produce more noise even if the dynamic range is fully supported by the camera, while the scene where the range is shifted upwards (or the aperture is larger) may produce clipping, and potentially additional noise in the mid-range, specific to WDR cameras.

It should be noted that the size of the aperture which limits the amount of light falling onto the sensor also affects the depth of field, the distance between the nearest and the farthest objects in the scene that appear acceptably sharp. So, there is a conflict between the desire to allow more light onto the sensor, which helps to reduce image noise and motion blur, and the need to get a sharper image. Less known is the fact that not only the aperture size is important but so is its shape. The conventional circular shape is not the best in terms of the power spectrum of spatial frequencies that it passes through.

The power spectrum of the circular aperture contains multiple zero-crossings that essentially filter out some content from the scene. There are less conventionally shaped apertures that produce a much better spatial response, and may even allow more light onto the sensor, however their usage requires a great deal of additional computation in image processing.

Multi-exposure method

Is there any way to go beyond the physical limitations of the image sensor that constrain the dynamic range of the camera? Fortunately, the answer is yes: the most popular approach is a multi-exposure method – two or more snapshots are captured at different exposure times (shutter speeds), and then composed into a single wide dynamic range image. Shorter exposures reveal scene details in the highlights while losing the details in the shadows, the longer exposures reveals details in the shadows while overexposing the highlights. The resultant WDR image is composed of pixels coming from both the short and the long shutter images: pixels from the short shutter image come primarily from the brighter parts of the scene, while pixels from the long shutter image(s) come primarily from the darker parts. Most WDR cameras use dual-shutter method, while some use triple and quadruple shutter technology to achieve a wider dynamic range.

Selecting the individual exposure durations and combining multiple individual snapshots into a single WDR image is where the technical difficulties are. The general goal in selecting the short shutter duration is to avoid clipping in the highlights, and to maximise the signal-to-noise ratio in the brighter parts of the scene. Clippings can be automatically be determined by the on-camera auto-exposure algorithm from the image histogram, as the camera adjusts the short shutter speed. Similarly, when selecting the long shutter speed the goal is to prevent dark clipping, which causes noise in the shadows.

Even though this approach appears to be straightforward, consider the less obvious implications. For example, depending on the scene itself, the brighter parts of the scene captured by the short shutter exposure may also contain less bright areas that are not dark enough to be ultimately replaced with pixels from the long shutter image in the final WDR image. Similarly, the long shutter image capturing the darker areas may contain less dark scene fragments that are not bright enough to be replaced by the short shutter pixels in the composed image.

As a result, these in-between areas of the scene may receive inadequate exposure – too long in the long shutter image, potentially causing overexposure of these areas, and too short in the short shutter image, potentially causing excessive noise in the affected areas. The effect of these exposure artifacts on the final WDR image manifests itself as signal-to-noise ratio discontinuity, and appears as areas of excessive noise around the middle of the dynamic range.

Limitations of WDR imaging

It should be noted that in some of the mass-produced WDR technologies, the choice of available shutter ratios is very limited due to certain technological and cost constraints. As a result, problems caused by selecting the inadequate shutter ratios become difficult to resolve, making noise and other artifacts highly dependent on the scene itself.

A further limitation of WDR imaging is related to motion artifacts. Due to different shutter speeds, parts of the scene that were moving at the time of capture will appear at different locations in the two (or more) individual snapshots that make up the composed WDR image. For example, consider a dark object that moves across a bright background scene. If the object was stationary, the dark pixels in the composed WDR image would come from the long shutter image, while the surrounding outline would come from the short shutter image. However, because the object is moving, its outline in the short shutter image does

not match its outline in the long shutter image.

A decision has to be made as to how to fill-in the mismatch. This becomes especially difficult when motion is accompanied by motion blur, which produces brightness values in-between the brightness of the object and the background. In the case of colour WDR imaging, motion artifacts may produce bright colour contours around the moving objects unless special computational measures are taken in image processing. Moreover, when excessive temporal noise is present, it could produce motion-like artifacts resulting in colourful noise patterns. Measures to suppress motion artifacts in WDR are known as motion compensation.

Motion compensation may produce visual artifacts in a special case of capturing WDR scene containing very bright artificially illuminated areas. Bright areas of the scene are captured primarily with the short shutter. If the duration of the short shutter is shorter than the duration of the half-cycle of artificial illumination (8.33ms in 60Hz countries, or 10ms in 50Hz countries), there could be significant local brightness variations between the short and the long shutter images. These variations may be mistaken by the on-camera motion compensation as legitimate motion, causing visual artifacts. In this scenario, disabling motion compensation may be a reasonable solution.

Displaying WDR video on a TV monitor

There are certainly special considerations in displaying wide dynamic range videos on a television monitor. Monitors are generally incapable of displaying wide dynamic range imagery; they are limited to a dynamic range, which is 200 to 300 times narrower than that of a typical WDR camera.

Fortunately, there is a solution: the problem is solved by taking advantage of one of the many idiosyncrasies of human visual perception, which places much more importance on local contrast variations, and much less on the global variations between the large areas making up the overall scene. To take advantage of this, the WDR image is put through a non-linear image processing process known as tone mapping, which reassigns pixel brightness values to achieve the reduction of global contrast while preserving the local one.

Consider a typical WDR scene in which the highlights correspond to the bright outdoor scenery while the shadows correspond o the indoor space. If the overall brightness range of the outdoor areas is significantly reduced to bring it closer to the overall brightness range of the dark indoor areas while preserving the local brightness variations in both areas, the overall appearance of the scene will remain perfectly acceptable to the human eye, while the image becomes displayable on a monitor.

Comparing performance of WDR cameras

It should be noted that tone mapping combined with the multi-shutter image capture is a highly non-linear process which may produce significant differences in the WDR image appearance even with relatively small changes in the scene. This makes it especially challenging, and requires a great deal of technical expertise, when comparing the performance of different WDR cameras. In particular, care must be taken to make sure that the fields of view, including their aspect ratios, are identical, and the apertures are the same.

Furthermore, it is important to always look at the entire captured WDR image, and not at a cropped fragment of it post-capture, for example, showing only the bright areas. This is because the appearance of the bright area in terms of its overall contrast, noise content, and its brightness may be entirely different depending on the content of the rest of the WDR scene. If there was a large dark area in the full scene, the appearance of the bright area will be significantly modified via tone mapping and via multi-exposure image capture in terms of its final contrast, brightness, and noise, as compared to a scene without a large dark area. Unfortunately, it has become a common practice to present WDR images cropped post-capture, which makes it impossible to judge camera performance.

Panoramic WDR

The combined effect of tone mapping and multi-exposure image capture becomes especially challenging when it comes to achieving a uniform panoramic image appearance in a multi-sensor panoramic WDR camera. Adjacent parts of the scene captured by individual image sensors may appear entirely different in terms of brightness, noise, and contrast, just because there is a slight change in scene content from sensor to sensor.

In order to produce a more uniform panoramic image, it is often necessary to sacrifice the dynamic range in some of the channels of the multi-sensor camera or perform an additional elaborate post-processing to equalise the appearance of the resultant multiple WDR images.

For more information, please visit:
www.arecontvision.com SST

How To Prevent More Of The Same Attacks To the Retail Sector

Article courtesy of Darktrace

Introduction

The retail sector has been hit by a series of cyber-attacks in the past few years, and even the largest companies are still falling victim. Tesco has suffered its second recent data breach, following a compromise of its online customers' data in 2013. Target now has the largest data breach in history to its name, with a subsequent attack on upmarket US retailer Neiman Marcus following hot on its heels. Why is this still happening?

We believe that organisations concerned about cyber security need to change their point of reference. At present, the centre of gravity is around the attack malware: how it works, how it is deployed, what it does, and how to deal with the subsequent post-incident clean-up process. The problem with this approach is that it is inherently slow and cumbersome, and some unfortunate organisation must suffer the effects of a zero-day attack before everybody else can benefit. This is an unsustainable position, especially given the well-documented scale of the threat.

The following paper is a study of the impact of point of sale (POS) malware incidents in the retail sector, the damage caused and how the current approach to cyber security is struggling to keep up with the threat.

We will explain why the Enterprise Immune System would have been able to spot the threats that manifested themselves on Target and Neiman Marcus's systems ahead of time, before those threats matured and turned into damaging attacks.

Common attack characteristics

Recent reported attacks on the retail sector, both in the UK and the US, have highlighted the difficulty that companies still have securing digital transactions in large, geographically diverse organisations, while combating the ingenuity, skill and agility of the cyber-crime community.

As details have emerged about recent incidents, including the attacks against Target and Neiman


OK
F1
F4
F2
C
F3

Marcus, it is illuminating to note a common set of characteristics that these data breaches share.

In each case:

1. The attackers used a variant of the BlackPOS malware, a specialised piece of software designed to be installed on POS devices, recording in memory all the data (both Track 1 and Track 2 data) from credit and debit cards

2. The attackers were believed to have been active in the corporate network for an extended period of time, probably months, using a number of compromised machines

3. Reports indicate that data harvested from the BlackPOS variant attack was stored locally (again in compromised infrastructure)

4. Reports also indicate that the stolen data stored in the compromised infrastructure was accessed repeatedly over an extended period to remove the 'significant' quantities of data

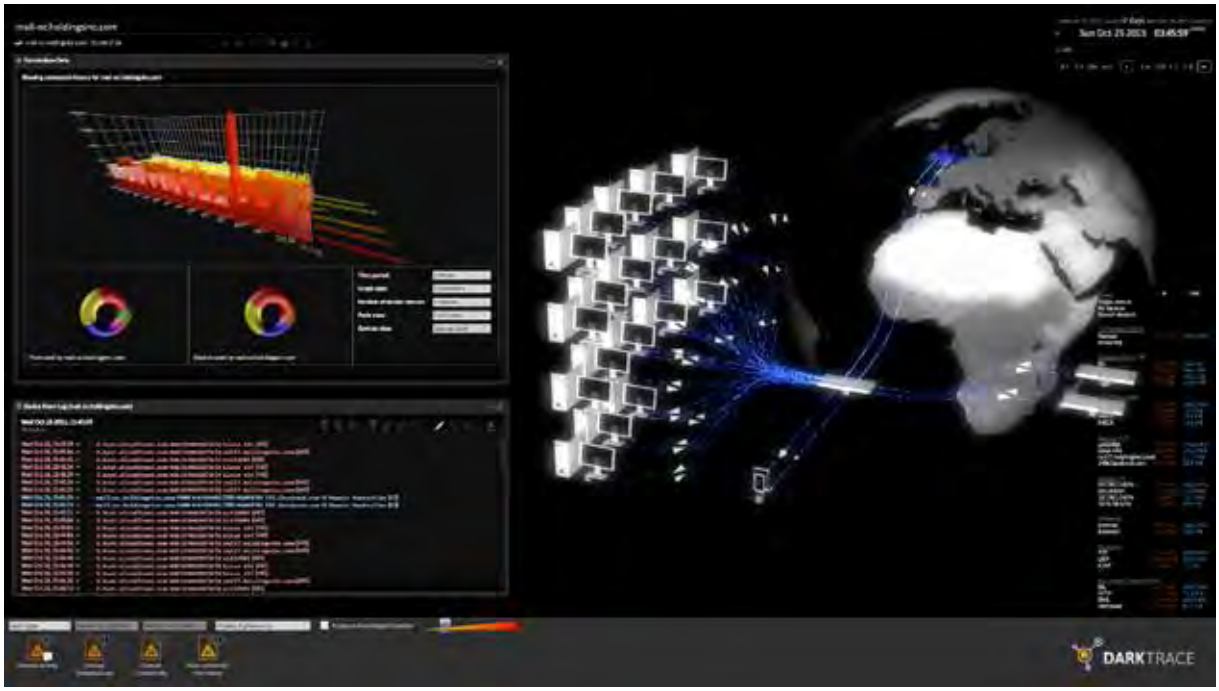
5. The attackers used a complex set of command and control, obfuscation (TOR), and data transfer repositories (FTP server) to finally exfiltrate the data from the target organization back to the attackers

6. The variant of BlackPOS used had been modified to "avoid detection and for use in specific environments," according to a source close to the Target attack

It is clear that approaching the problem of retail cyber-crime as a traditional cyber security issue is not working. Why is that?

The defender is lagging behind

Cyber-criminals have a development cycle of code creation and subsequent modification, which is measured in minutes. An extensive network of users can rapidly self-organise on the Internet for mutual benefit. Limitations in experience, code capability and understanding can be overcome by sub-contracting to like-minded individuals extremely quickly and efficiently. The rising number of cyber-crime 'information exchange' web sites in the 'dark internet' is testimony to this growing and sophisticated hacker community.
Meanwhile, on the defense side, it takes a finite amount of time to forensically examine any attack. The details emerge slowly, and the companies affected are naturally reluctant to lay bare, in public, the full details of any attack. Therefore, the details of the signature or rule required to stop a similar attack take a certain amount of time to transfer into the cyber security community and – potentially – even longer to get into existing security



products in order to protect companies against similar attacks in the future. Legacy, rules-based security tools are constantly running to catch up with yesterday's attackers.

Targeting the weakest link

Investigations in the aftermath of the Target cyber-attack, which saw 40 million credit and debit card numbers and the personal information of 70 million customers stolen, have revealed the sophistication of the attackers and the depth of the intrusion. Yet the way the attackers got into Target's systems in the first place was textbook. They struck at their target's weakest point – in this case, its supply chain.

It has been revealed that Target hackers gained access to the leading retailer's systems via a refrigeration contractor – one of the many suppliers that connected to Target's systems. Fazio Mechanical Services Inc. helps install and maintain refrigerators for various supermarket chains – amongst them Target. The contractor was linked remotely to Target's computer systems for electronic billing and contract submission.

Having infiltrated Fazio and stealing user credentials, the hackers went on to infiltrate Target's systems and carried out one of the largest and most damaging data breaches on record – without triggering any antivirus or other security software.

Locking out suppliers

The revelation of how the hackers managed to get into Target has provoked criticism of the retailer's security procedures. Target faces a slew of legal actions related to the breach of consumer data – customers and banks have filed 68 class action suits. It has been claimed in such legal suits that Target did not take proper steps to protect its customers' information. "It's time to reassess the kind of information that they [suppliers] have access to," one attorney suggests.

Such comments betray a misunderstanding of the reality of modern business and global networks. Business in the Internet age has all been about sharing information with the world and enabling more connections and collaboration between parties that work together. Networks are interconnected by nature, not isolated silos of information. The upside of this interconnectedness has been immeasurably large; however, it inevitably involves allowing access to any number of relevant external entities – contractors, suppliers, freelancers, your employees' personal devices, etc. Trying to fight this trend is hopeless, and implying that networks can simply be 'secured' against all possible vulnerabilities is either disingenuous or plain naïve. It is clear that border control does not work when your network border extends up your supply chain.

The reality is that large global corporations need to be connected to their suppliers to work efficiently and stay competitive. But they cannot be expected to vouch for the security of every single one in the supply chain. Fazio had access to Target's systems in order to send contracts and invoices to Target more efficiently and manage joint projects. In the same way, a Target employee would have access to various parts of the network according to his or her job function. Despite all the security training and certification in the world, both entities represent vulnerability. Edward Snowden has reminded us all that external threat is not the only thing we should worry about.

No retailer, whether large or small, can remove threat from its systems and networks.

Hiding in the noise

What is interesting about the Target attack is not how the attackers got in – this was relatively trivial. The interesting part is the behavior that they manifested as they carried out their multi-stage attack from within the network.

Target's attackers were no amateurs. The malicious computer code used against the retailer's credit-card readers, which was partly written in Russian, included additional features that were designed to hide the fact that copies of the customer data were being collected from the magnetic stripes on Target's customers' payment cards. The information was carefully concealed within one of Target's own servers before being exfiltrated outside the organization. The virus deliberately carried out the theft of the credit-card data during prime business hours to hide itself in the noise of normal business interactions, between 10 am and 5 pm.

The preparation stages are the highest-risk part of an attack – they take time, require ingenuity to avoid detection and entail acting in a way that is, by nature, abnormal. Yet Target's hackers successfully pulled it off, stealing millions of records – at the deepest level of its target organisation – without triggering any of the

security tools that were in place precisely to protect the retailer from this scenario.

Intelligence-based approach

It may be impossible to keep threat locked out of your systems, but better defense to spot advanced attackers, such as those that caught Target out, is possible if we shift our focus to the behavior that the adversaries manifest once they have landed on the target network. It is here where the real sophistication of the attack comes into play, as the attacker carries out the various stages of its mission – each strategically designed to reach their goal.

These attackers were good at hiding themselves from anti-virus tools, rules-based security software and network administrators. When they did take action, their movements were subtle, traversing the network and identifying their target data conspicuously so as not to attract attention. Yet they acted in ways that were, by definition, abnormal in some way, given the normal activity of the network and its users.

How Darktrace would have spotted the evolving threat?

Darktrace's self-learning Enterprise-Immune System technology, based on pioneering new mathematics, detects emerging threats as they manifest themselves on the network, by joining up weak indicators of abnormality and spotting truly anomalous behavior representing threat. As an appliance, it can be utilised in multiple parts of a company's networks.

As details of the exact nature of recent attacks are emerging, it is possible to observe that, with its complex mathematical models of networks, devices and users, the Darktrace platform would have been able to deliver advanced notice of the evolving attack.

Let us assume that the Darktrace Enterprise Immune System was implemented and had visibility of both the corporate headquarters and remote, customer-facing facilities of one of the recently hit retailers, such as Tesco or Target.

Studying the recent attacks in depth, it can be seen that there were numerous anomalous network connections taking place between various networked machines across the extended enterprise. The Darktrace Enterprise Immune System would have detected anomalous behavior in multiple stages of the attacks.

What Darktrace would have detected?

Based on known information about recent attacks on retailers, we may observe that Darktrace would have spotted:

- Abnormal activity around the originally compromised machine in the early stages of the attack planning
- Unusual connections between POS terminals and compromised hosts
- A considerable volume of data being moved between unusual machines within the corporate network
- As the data amassed in those compromised hosts, the movement of data from the corporate infrastructure, via the Internet, into a foreign-hosted FTP site.

Darktrace's unique approach, powered by Enterprise Immune System technology, would have allowed for the detection of numerous anomalies as the threat developed within the organizations. By mathematically modelling 'normal behavior' for the organization as well as each user and device, Darktrace would have allowed for the mitigation of the live threat as it evolved – not just after it had stolen the goods and the damage was done.

Conclusion

The challenge to retailers is only getting bigger. The FBI detected 20 hacking cases in the past year, and has formally warned US retailers that they expect more to come in a report published in January 2014. UK retailers are similarly bracing themselves for more of the same.

"It's an on-going tale, one that is constantly moving," says Andrew Rose, principal analyst for security and risk at Forrester Research. "But from the outside it looks like nothing much has changed." Something has to change fast, if we are to stop our personal details flying off retailers' servers into the hands of criminals, and avoid the destruction of well-earned trust in our most cherished retail brands.

The retail industry urgently needs to hit the reset button, and shift from its default position of damage control and investigation, to a proactive, intelligence-based approach. This means it needs to stop chasing after the latest malware exploit and get ready for fighting the threat on home territory – and winning.

For more information, please visit:
https://www.darktrace.com/ SST

RF/RFID Antenna E10 2.0 Boasts Flexible Design Options And Powerful Use of Data

The E10 2.0 comes in both RF and RFID versions to meet the specific needs of retailers and enables them to future proof their business investments. For example, by allowing retailers to invest in RFID at a later point via an RFID upgrade kit, the E10 2.0 enables them to use their existing electronic article surveillance (EAS) RF solutions today and then use RFID when the time is right for their businesses. In dual-mode, only one tag is required for both inventory management and loss prevention.

Flexible Design

- The antenna can be used as a sleek see-through acrylic design, or can be changed instantly to become an advertisement panel for a store's products, simply by inserting graphic panels that are held in place by the elegant standard display.
- The new antenna also is EMOPrint ready, which means retailers, can obtain from Checkpoint full color textile panels that are easy to modify on the E10 2.0.
- Retailers can further customise the antenna by ordering from Checkpoint full color graphic prints that are applied to the antenna base plates and RFID elements, to create a unique branded antenna solution.

Powerful Data Analytics

- Integrated Visitor Counting is embedded in the new system, offering highly sophisticated functionality, analytics and reporting to improve profitability.
- Integrated with EVOLVE-Store, a real-time app for smartphones and tablets that supports real-time EAS and organised retail crime (ORC) event management, create a powerful data-centric solution.
- The improved RFID functionality of E10 2.0 will help loss prevention managers better understand what is potentially stolen, and store associates improve stock management by having the right product at the right time.

For more information, please visit: http://us.checkpointsystems.com/ SST

MicroEngine®
Integrated Security Systems

MicroEngine's POE Powered Encrypted IP One Door Access Controller

MicroEngine is the trusted brand in Integrated Security Solutions in Malaysia and Singapore, which has plenty of experience in many large-scale projects, in both private and public sector. MicroEngine is launching the POE powered Encrypted IP One Door Access Controller P1000i with an onboard integrated POE power supply circuit with charger and dedicated Fire Alarm Input.

People are more sensitive to environment impact on the things that they do now, and are more interested in using greener products. In security system, Power over Ethernet (PoE) is one of the solutions to this. PoE is a technology that provides both data and power connections in one cable. Doing so minimises the number of wires that must be strung in order to install the network and power. Hence the result is more cost effective, less downtime, easier manageable and maintenance, better configurability and greater installation flexibility than with the traditional wiring. We are now offering Power over Ethernet (PoE) on our access controller – P1000i.

Our P1000i POE Access Controller supports our in-house PLATO readers on RS485 connection, which gives you the options of multiple mode of reader only, reader + keypad or a reader + keypad + color LCD operation, which means the door, can be configured to operate on different entry access mode at any time. It has 4 supervised inputs, 1 for door sensor, 1 for push button. The other 2 are general purpose inputs which can be used as alarm input or event triggered input. It has built in DEDICATED Tamper Switch input and Fire Alarm input for higher standard requirements. Also, the IP communication is encrypted with AES128 with dynamic key exchange to increase the security. P1000i supports both push and pull communication methods.

On top of this, it provides 2 Wiegand / ABA reader inputs that support 64 bits card numbers for better security, the more digits it can read, the lower possibility of reading duplicate card number. This will reduce the chances of card number duplicates in large card based installation. P1000i supports up to 10,000 card user database and 50,000 transaction records. Our reader, the PLATO reader, has the options of Prox, Mifare and Mifare DESFire.

For more information, please visit: http://www.microengine.net SST

Model: Advantech Industrial 4U Hybrid Intelligent Video System ACP-4000VS

By: Advantech Co. Singapore Pte Ltd
ⓘ www.advantech.com

- Industrial grade intelligent surveillance system with flexible hybrid system structure
- Free bundled VMS/CMS and SDK for AP software integration
- Free bundled and optional intelligent video analysis (IVA) software
- Supports analog/digital/IP Cameras with Hybrid structure
- 3 TB HDD for 16-channels of recording for 15 Days (D1@240FPS)

Model: SurroundVideo G5

By: Arecont Vision
ⓘ www.arecontvision.com

- Includes a 5 megapixel resolution model with STELLAR (Spatio TEmporal Low Light Architecture) advanced low light technology for best-in-class light sensitivity to capture more detail
- Standard and smaller form factor versions of 12MP and 20MP SurroundVideo G5 cameras each delivering double the frame rate of previous models will be available soon
- Enhancements for the standard and smaller form factor models include an option for Wide Dynamic Range (WDR) at 12MP resolution to capture useable video in scenes with highly contrasted lighting
- The standard form factor model offers P-iris lenses and remote focus. The SurroundVideo G5 12MP and 20MP models offer pixel binning for increased sensitivity in low light applications
- Features an IP66-rated environmental housing and a polycarbonate bubble that is 1K-10 rated impact-resistant
- The new black gimbal offers enhanced aesthetics

Model: SD-3030 Speed Dome Camera

By: OvisLink (AirLive)
ⓘ www.airlivesecurity.com

- Built-in Smart Tracking Function
- Up to 30x optical zoom
- Up to 30fps @ 3 Megapixel and 60fps @ 1080p Full HD
- Auto and manual PTZ calibration
- Wide Temperature Range: -40 degree Celsius - 50 degree Celsius
- 3D Noise Reduction
- Defog function
- Backlight compensation

Model: AVENTURA CAM-IPM-8ZA SERIES

By: AVENTURA TECHNOLOGIES INC.
ⓘ www.adventuracctv.com

- 8 Megapixel (4K)
- 1/1.8" Progressive Scan CMOS
- Up to 36x Optical Zoom
- Auto-Tracking
- H.264 / MPEG4 / MJPEG
- AC 24V / PoE
- ONVIF / PSIA / CGI Compliant

Model: C260

By: Shenzhen LSVT Co., LTD
ⓘ www.lsvt.com.cn

- Private CCTV camera housing support OEM
- Support every solution: HD CVI/TVI/AHD/IP/ CMOS
- Support every lens: fixed lens/vari-focus lens/ motorised lens
- Support different colour: red/black/blue/grey
- Support brand exclusive agency for 1 country
- Support 25 - 30m IR distance
- IP66

Model: GOB-300Np Star-LTE

By: Brickcom Corporation
ⓘ http://www.brickcom.com/

- Built-in LTE module and SIM slot for Wireless Connectivity
- i-Mode for Different Environments
- i-Stream Technology - Intelligent Storage Space Saver
- Sony STARVIS 3M Outdoor Bullet Camera, Support Video Quality 3M @ 30fps Streaming
- IK10 & IP67 Outdoor enclosure built-in fan (-70 degree Celsius – 60 degree Celsius) and Heater
- SmartFocus to focus remotely and rapidly
- Smart IR to get better illuminated image
- Built-in Micro SD / SDHC / SDXC Memory Card Slot for local storage

Model: EPTZ9300

By: EverFocus Electronics Corp.
ⓘ www.everfocus.com.tw

- AHD Resolution 1080p / 720p and SD output
- 30x optical zoom lens
- UTC & RS-485 communication function
- 16 Cruise Tours can be set, and each Tour contains up to 16 Positions
- OSD Function
- IP66
- Privacy Zone Masking
- Tilt Angle: 220 degrees (Auto Flip)

Model: 2Mp Full HD 12x Mini Network PTZ Dome Camera (SD40212T-HN)

By: Dahua Technology Co. Ltd
www.dahuasecurity.com

- Powerful 12x optical zoom
- Support dual-streams encoding
- Maximum of 25/30fps@1080P(1920´1080) & 50/60fps@720P resolution
- WDR, Day/Night (ICR), DNR (2D&3D), Auto iris, Auto focus, AWB, AGC, BLC
- Max 300 degrees per second pan speed, 360 degrees continuous pan rotation
- Up to 300 presets, 5 auto scan, 8 tour, 5 pattern
- Built-in 2/1 alarm in/out
- Support intelligent 3D positioning with DH-SD protocol
- IP66 (outdoor), IK10 (optional), POE+

Model: GTC-284 - 4 Megapixel FULL HD Network IR CCD Camera

By: Global Top Technologies (M) Sdn Bhd
www.gtc.my

- Optional fixed lens: 4/6/8/12 mm
- H.265/H.264 & MJPEG dual-stream encoding
- 2pcs /4pcs 42mil IR LED Array
- IP66 rating
- IR LED Module (Distance up to 40m)
- DWDR, Day/Night (ICR), 3DNR, Auto Iris, AWB, AGC, BLC
- ONVIF 2.3 supported
- Dimension: 353mm x 119mm x 98mm
- Weight Camera: 850g

Model: WebEntra Compact Series IP Access Controller

By: ASIS Technologies Pte Ltd
ⓘ www.asis-technologies.com

- Cost-effective, web-based, modular access control solution comprising
- C302 Two-Door IP Access Controller (Master Module)
- C312 Two-Door IP Access Controller (Slave Module)
- Complete 2 door access control and online monitoring
- "InstaSTART" Advanced Plug & Play Technology
- Supports up to 64bits CardIDs, compliant to ISO14443A/B
- Supports PoE (IEEE802.3af) and PoE+ (IEEE802.3at)
- Supports a maximum of 20, 000 cardholders and 50, 000 event capacity

Model: FV Multibio

By: Dytronic
ⓘ www.dytronic.com

- The first Multimodal FingerPrint & FingerVein device in the world with the combination of multitouch screen for enhanced interactivity for time attendance and high security applications
- FV multibio can be loaded with unmatched combined functionalities including but not limited to built-in camera, microphone, speaker, 3G, WiFi, Bluetooth, lithium battery, RFID (NFC, Mifare, HID), USB flash, micro SD, IP 65, gorilla glass protection and PoE
- Server connecting to real IP of device and device connecting from within private networks back to the server
- Access controller functionality in small factor such as door sensors, scheduled release of doors, smart backup battery switching between secure or operation mode in case of power failure and no reported attacks
- Database encryption in extreme security use
- Camera for added security or even adding a third biometrics like facial recognition
- Intercom with two-way communications using IP networks

Model: BQT Cobalt YD30

By: BQT Solutions (SEA) Pte Ltd
ⓘ www.bqtsolutions.com

- Door misalignment of +/-8mm is automatically corrected
- Releases instantly when requested even with 100kg side load on the door
- Less than 50mA standby current
- Monitoring of both Door and Bolt positions
- Voltage input of 12 – 24VDC can be supplied
- On site conversion from Fail Safe to Fail Secure
- Stainless Steel parts are used throughout the lock
- Holding force of 10,000N with two automatic dead bolting pins.

Model: Architect Blue - Bluetooth Smart

By: STid
ⓘ www.stid.com

- 4 identification modes for an intuitive, fluid and easy access management: Card, Remote, Slide & Pass and Tap Tap modes
- Easy deployment, using a mobile application, with offline and online management to configure credentials and load access rights
- High Security management: EAL5+ secure data storage, secure exchanges between the reader and the smartphone, multi-factor authentication (PIN code, biometrics
- Fully interoperable, supporting the main Operating Systems: Android, iOS and Windows Phone
- Multi-technologies combining RFID, Bluetooth Smart (Low Energy) or NFC HCE technologies
- Fully customisable readers: company logo printings, casing colour or cover

Model: The Guardian Road Blocker

By: ATG Access Limited
ⓘ www.atgaccess.com

- Market leading, crash tested and cost effective road blocker
- Successfully impact tested withstanding a 7, 200k vehicle travelling at 80kph
- No large above ground cabinets required as a small integral pump is utilised to raise and lower the blocker
- Shallow foundation product only requiring 400mm of depth to install
- Installation is straight forward only requiring a single concrete pour and a standard rebar structure
- Modular design reducing the cost and difficulty of transportation.
- Incredibly easy to service and maintain
- Able to withstand heavy vehicles driving across the product on a day-to-day basis when in the lowered position and still remain fully functional

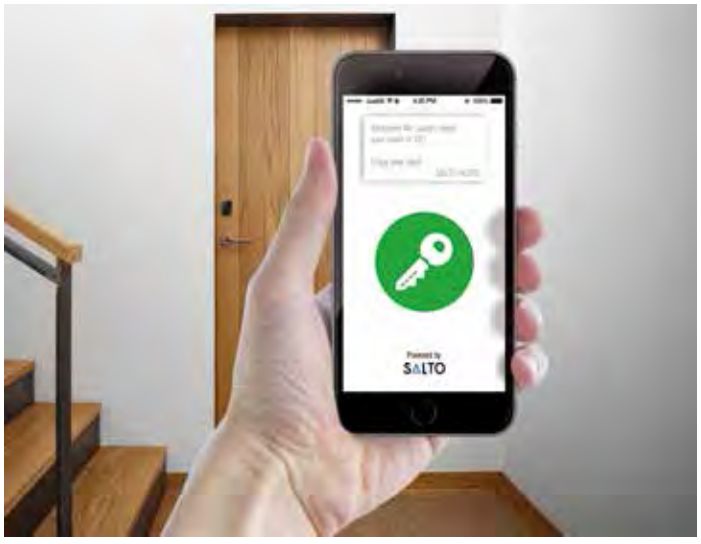
Model: MAG AR500U

By: Magnet Security & Automation Sdn Bhd
ⓘ www.magnet.com.my

- Dualtec RFID technology capable to penetrate premium solar film (Vkool Elite) in the market to achieve 1.8 to 7 metre range
- Affordable "Long Range" reader for "High Speed" parking access solution
- Card can be removed from transponder to be used inside the building – true "One-Card" solution for outside parking and inside door access
- Support EM (125Khz) or Mifare (13.56Mhz)
- Absolute directional 60 degree angle reading range to avoid unintended wrong reading of car following behind or beside
- Integrated with MAG BR618 fast speed barrier to achieve 1.8sec opening with 4 metre arm
- Fully integrated hardware and access control software solution
- Spare part and repairing services available locally

Model: JustIN Mobile Solution

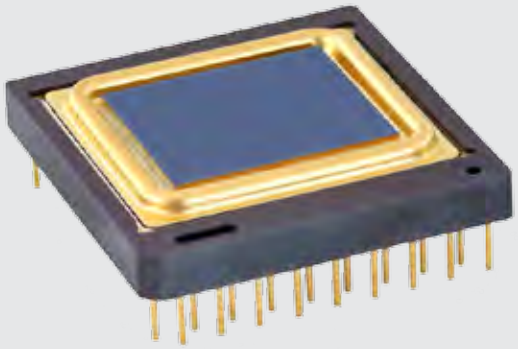
By: SALTO Systems
ⓘ www.saltosystems.com



- JustIN Mobile app enables users to receive keys online, anytime and anywhere.
- Compatible with the SALTO XS4 escutcheons range.
- Computer managed through SALTO ProAccess SPACE software.
- Enables access rights to be changed or extended instantly and remotely.
- Works with iOS and Android smartphone devices.
- Encrypted data transfer between phone and lock means secure authentication.
- AES 128 bit communication and secure opening procedure with key securely encrypted.

Model: Pico640 Gen 2 (TM), thermal image sensor

By: ULIS
ⓘ http://www.ulis-ir.com/



- Compact, lightweight and energy efficient Pico640 Gen 2 delivers enhanced image quality, proven reliability and ease of use
- Outstanding battery life
- Unrivalled robustness
- Spectral response: 8 - 14 μm
- HSynch/VSynch clocking
- I^2C serial link for register programming
- Maximum frame rate 120 Hz full resolution
- Overall dimension (mm): 24.13 x 24.13 x 4.14 pin out excluded
- Weight < 6.5 g

Model: Checkpoint RF/RFID Antenna E10 2.0

By: Checkpoint Systems, Inc.
ⓘ http://us.checkpointsystems.com/

- The antenna can be used as a sleek see-through acrylic design, or can be changed instantly to become an advertisement panel for a store's products, simply by inserting graphic panels that are held in place by the elegant standard display
- The new antenna also is EMOPrint ready
- Retailers can further customise the antenna by ordering from Checkpoint full color graphic prints that are applied to the antenna base plates and RFID elements
- Checkpoint's data analytics for the E10 2.0 help merchandising and operations staff better understand store traffic
- Integrated Vistor Counting is embedded in the new system, offering highly sophisticated functionality, analytics and reporting to improve profitability
- Integrated with EVOLVE-Store, a real-time app for smartphones and tablets that supports real-time EAS and organised retail crime (ORC) event management
- The improved RFID functionality of E10 2.0 will help loss prevention managers better understand what is potentially stolen

Model: VeriFire

By: GKB Security
ⓘ www.gkbsecurity.com

- 1080P CMOS Megapixel Sensor
- ONVIF 2.0 Compliance
- 4 video streams
- Waterproof (IP 66)
- Two-way audio
- DI / DO
- ROI
- 3DNR
- Flame & Smoke Detection

Model: FlexZone

By: Senstar
ⓘ www.senstar.com

- Detect and locate perimeter intrusions over a distance of up to 600 m
- Pinpoint intrusions with +/- 3 m (10 ft) accuracy
- Flexible software-based zoning (up to 60 distinct zones per processor)
- Power and data over sensor cables simplify infrastructure requirements
  Communication path redundancy ensures continued perimeter protection in the event of a cable cut
- Software - configurable output relays simplify integration with alarm monitoring systems
- Optional Ethernet card with Power over Ethernet (PoE) capability
  Wireless gate sensor option eliminates challenge of cable installation and maintenance on swinging and sliding gates

Model: D-TECT IP range

By: GJD Manufacturing Ltd
www.gjd.co.uk

- Range of External Quad PIR and Dual Technology IP detectors
- Seamless integration with VMS providers and CCTV systems
- Programmable detection ranges up to 50 metres
- Remote access via a user-friendly, web based interface to enable remote monitoring from anywhere and at any time
- Uses Power over Ethernet, advanced signal processing, quad pyro and optical systems
- Robust IP65 zinc metal housing
- Low maintenance and cost efficient

Model: Industrial EN50155 Ethernet Switch - ITP-G802SM-8PH24

By: CTC Union Technologies Co., Ltd
ⓘ www.ctcu.com

- 8x 100/1000Base–T (M12) + 2x100/1000Base–X SFP with 8x PoE+ Managed Ethernet Switch
- IP67 grade housing for against water, dust, and oil
- 24/48VDC redundant dual input power, and built-in power booster design up to 55 VDC for PoE output
- Regulated PoE output voltage (55VDC) to stabilize PoE device, and guarantee delivery PoE power distance to 100 metres
- UL60950-1, EN50155, EN50121-4, EN61000-6-2, EN61000-6-4, CE, FCC certification
- Provides SmartConfigTM for quick and easy mass configuration tool
- Supports SmartViewTM for Centralised Management
- SNMP, Web, Telnet, CLI, IPV6, DHCP, RMON, MIB II, QoS, CoS, Security, IGMP, VLAN, LACP, IEEE1588 V2

Model: Intellect Enterprise PSIM

By: Axxonsoft Asia Pte Ltd
ⓘ www.axxonsoft.com

- Open-Platform distributed multi-functional PSIM solution
- Allows connecting CCTV, access control, fire/security alarm, and perimeter security infrastructure to unified intellect command & control environment
- Integrate diverse hardware equipment into a single platform regardless of brands and models
- Flexibility to integrate with other subsystem with includes video content analysis, facial recognition, license plate recognition and as an integrated solution
- Indefinite scalability and modular architecture
- Powerful macros & scripts to automate the response mechanism according to the events
- Support OPC, Bacnet, ONVIF and other standard industry protocol, which makes the integration hassle-free
- Incident Management and Real-time Automated Response methodologies
- Customisable interface - On-line reports and tracking with strong authentication

TRADE CONNECTION

Home page annoucements for added business opportunities.
Register now, contact:

Tel: (65) 6842 2580 Fax: (65) 6842 2581 / 6745 9517
E-mail : info@tradelinkmedia.com.sg

This space could be yours for

US$				Color
1x	3x	6x	9x	12x
500	440	380	320	260

S$				Color
1x	3x	6x	9x	12x
775	682	589	496	403

building (Southeast Asia)
Sustainable Architecture • Interior Design • Landscaping

Asia-Pacific's leading source of information for professionals interested in the technique and technology of quality architectural, interior and landscaping design.

CONSTRUCTION (Southeast Asia)

Features civil and structural projects in the region and all over the world, the latest in construction equipment, materials, technology and industry news.

Security Solutions Today

Showcasing products in categories that include access control, CCTV/ surveillance systems, integrated security systems, detection and alarm systems, fire extinguishing systems and passive fire protection.

lighting today

A publication that aims to promote lighting's purpose as an integral part of realising a quality built environment, emphasising the importance of the role of professional lighting designers in the total design process.

bathroom +kitchen today

A regional trade magazine designed to reach a progressive, diverse and dynamic audience of the bathroom, kitchen and ceramic industries.

LAVA
Lighting Audio Visual Asia

With a solid network of designers, installers, specifiers and rental specialists in the lighting, audio, and visual solutions industries, LAVA has what it takes to place your brand in the spotlight.

Scan to visit our website

TRADE LINK MEDIA PTE LTD
101 Lorong 23, Geylang, #06-04, Prosper House Singapore 388399 T: (65) 6842 2580 F: (65) 6745 9517
W: www.tradelinkmedia.com.sg E: info@tradelinkmedia.com.sg

Model: BioSurveillance NEXT

By: Herta Security
ⓘ www.hertasecurity.com

- Immediate identification of subjects in crowded environments and in constant movement
- Analyses multiple cameras simultaneously
- Fully automatic and non-invasive technology
- Works properly on changes of facial expression, illumination, beard, eyeglasses, scarfs and caps
- Automatic subject enrollment
- Allows for multiple watch lists (e.g. blacklist, VIPs, etc.)
- Alarms can be visualised on remote mobile devices

Model: PD1041 Hardened Surge Protection Device–RJ45

By: EtherWAN Systems, Inc.
ⓘ www.etherwan.com

- Provides pair-to-pair voltage surge protection through RJ45 connector
- Supports DIN-rail or desktop installation
- Wide temperature operation range from -40 degree Celsius to +75 degree Celsius
- Compatible with 10/100BASE-T, Gigabit and PoE products with pass-through data and PoE power
- Compliant to UL497B
- Protects your valuable network equipment
- SPD with RJ11/terminal block connector coming soon

Subscription Form

Fax your order today
+65 6842 2581

(Please tick in the boxes)

Southeast Asia Building

SINCE 1974

☐ 1 year (6 issues)

Singapore	S$45.00
Malaysia / Brunei	S$90.00
Asia	S$140.00
America, Europe	S$170.00
Japan, Australia, New Zealand	S$170.00
Middle East	S$170.00

Bathroom + Kitchen Today

SINCE 2001

☐ 1 year (4 issues)

Singapore	S$32.00
Malaysia / Brunei	S$65.00
Asia	S$80.00
America, Europe	S$130.00
Japan, Australia, New Zealand	S$130.00
Middle East	S$130.00

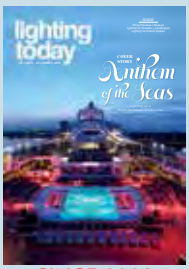
Southeast Asia Construction

SINCE 1994

☐ 1 year (6 issues)

Singapore	S$45.00
Malaysia / Brunei	S$90.00
Asia	S$140.00
America, Europe	S$170.00
Japan, Australia, New Zealand	S$170.00
Middle East	S$170.00

Lighting Today



SINCE 2002

☐ 1 year (4 issues)

Singapore	S$32.00
Malaysia / Brunei	S$65.00
Asia	S$80.00
America, Europe	S$130.00
Japan, Australia, New Zealand	S$130.00
Middle East	S$130.00

Security Solutions Today

SINCE 1992

☐ 1 year (6 issues)

Singapore	S$45.00
Malaysia / Brunei	S$90.00
Asia	S$140.00
America, Europe	S$170.00
Japan, Australia, New Zealand	S$170.00
Middle East	S$170.00

Lighting Audio Visual Asia

SINCE 2013

☐ 1 year (4 issues)

Singapore	S$32.00
Malaysia / Brunei	S$65.00
Asia	S$80.00
America, Europe	S$130.00
Japan, Australia, New Zealand	S$130.00
Middle East	S$130.00

IMPORTANT Please commence my subscription in _____ (month/year)

Personal Particulars

NAME: _____

POSITION: _____

COMPANY: _____

ADDRESS: _____

_____

TEL: _____ FAX: _____

E-MAIL: _____

Professionals (choose one):

☐ Architect ☐ Landscape Architect ☐ Interior Designer ☐ Developer/Owner

☐ Property Manager ☐ Manufacturer/Supplier ☐ Engineer ☐ Others

☐ I am sending a cheque/bank draft payable to:

Trade Link Media Pte Ltd, 101 Lorong 23, Geylang, #06-04, Prosper House, Singapore 388399

RCB Registration no: 199204277K * GST inclusive (GST Reg. No: M2-0108708-2)

☐ Please charge my credit card (circle one): Amex / Diner's Club

Card Number: _____ Expiry Date: _____

Name of Card Holder: _____ Signature: _____

ADVERTISERS' INDEX

The 14th Asian International Security, Safety and Fire Protection Show & Conference

Co-located with

Build Asia

The Technology Showcase for the Building, Electrical Engineering and Security Industries

4-6 MAY 2016

Hong Kong Convention & Exhibition Centre

Contact Us Now to BOOK YOUR PRIME LOCATION!

www.AsianSecuritex.com

Organiser

Hong Kong Exhibition Services Ltd
+ 852 2804 1500
exhibit@hkesallworld.com
Ms Karina Yu

ALLWORLD EXHIBITIONS MEMBER

follow us

Build4Asia

OVER 30,000 BUYERS AND BUSINESS PARTNERS UNDER ONE ROOF

@IFSEC #IFSEC

IFSEC International

SECURING PEOPLE, PROPERTY & ASSETS

21-23 June 2016, ExCeL London

Access the latest technology to find the perfect solution to your business needs

The global stage for security innovation and expertise

- See over 600 secuirty solution providers all in one place
- Free education provided allowing you to learn from industry leaders
- Experience the latest gadgets for the first time along the Innovation Trail
- Be productive and pre-book meetings with your preferred suppliers

PART OF PROTECTION & MANAGEMENT 2016
UNITING PROFESSIONALS ACROSS SECURITY, FIRE, SAFETY, FACILITIES & SERVICE MANAGEMENT

GUARANTEE YOUR PLACE AND REGISTER NOW AT IFSEC.CO.UK/SECURITY

Supported by

bsia · NSI Security. Improved · ASIS · IPSA

Organised by

UBM