Security Solutions Today

March / April 2016

HEALTHCARE SECURITY

Cover Focus Security Trends In The Healthcare Industry – New Risks And Priorities For Keeping Patient Information Safe

Inside Look Physical Identity Access Management Systems Prescribed For Hospital Safety And Security Wellness

Security Feature Sony – In Focus Security Demands For Emerging Markets In ASEAN & More!

Show Preview What's In Store For Secutech 2016!

Scan this code to visit our website

dahua TECHNOLOGY

Eco-Savvy Series 2.0

4-Megapixel IP Camera

- 4Mp@20fps; 3Mp@25/30fps
- Triple streams supported
- IP67, IK10 Protection
- Smart video detection
- True WDR up to 120dB
- 30x optical zoom(PTZ camera)

4Mp | 1080p FULL HD | ICR D/N | IP67 | PoE | IK10

Recommended models:

>> IPC-HFW5121/5220/5221/5421E-Z <<
>> IPC-HDBW5121/5220/5221/5421E-Z <<
>> IPC-HDBW4120/4220/4221/4421E <<
>> IPC-HDBW4120/4220/4221/4421F <<
>> SD59212T/220T/230T-HN (2MP) <<
>> SD50220T/230T-HN (2MP) <<

CE FC UL RoHS ISO 9001:2000

www.dahuasecurity.com

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

secutech TAIPEI
SECUTECH TAIPEI 2016
19 – 21 Apr 2016 Taipei, Taiwan
Booth: NO.4129

Our focus is making professional video surveillance easy for everyone

We are constantly searching for ways that ease installation. Our DINION IP 4000 and DINION IP 5000 bullet cameras are engineered for outdoor locations where first-time-right installation is particularly important. Both cameras are simple to install with a dedicated surface mount box and enable a dust and watertight installation. Set up is also easy thanks to Automatic Varifocal. **Learn more at www.boschsecurity.com/hdsecurity**

BOSCH

Invented for life

CONTENTS

March-April 2016

Security.

At the Center of Your Business.

Genetec Security Center is the leading enterprise-class security platform deployed by some of the world's most demanding organizations, governments and cities.

From video surveillance and license plate recognition to access control and intrusion detection, Security Center unifies the security systems that are critical to your operations, so you can see the big picture and make better security decisions – both today, and tomorrow.

Start Here. At Your Security Center.

Learn more at
genetec.com/mysecuritycenter

Video Surveillance | Access Control | Automatic License Plate Recognition

genetec.com

Genetec
Innovative Solutions

CONTACTS

March-April 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
Belle Choong (belle.choong@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: Axis Communications
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)

The magazine is available free-of-charge to applicants in the security industry who meet the publication's terms of control. For applicants who do not qualify for free subscription, copies will be made available, subject to the acceptance by the publisher, of a subscription fee which varies according to the country of residence of the potential subscriber in the manner shown on the right.

The editor reserves the right to omit, amend or alter any press release submitted for publication. The publisher and the editor are unable to accept any liability for errors or omissions that may occur, although every effort had been taken to ensure that the contents are correct at the time of going to press.

The editorial contents contributed by consultant editor, editor, interviewee and other contributors for this publication, do not, in any way, represent the views of or endorsed by the Publisher or the Management of Trade Link Media Pte Ltd. Thus, the Publisher or Management of Trade Link Media will not be accountable for any legal implications to any party or organisation.

Views and opinions expressed or implied in this magazine are contributors' and do not necessarily reflect those of Security Solutions Today and its staff. No portion of this publication may be reproduced in whole or in part without the written permission of the publisher.

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

Each Out-of-Stock Situation is a Lost Sale.

Checkpoint Systems is your partner for Merchandise Availability Solutions:

- ❑ Increase your Sales
- ❑ Maximize On-Shelf Availability
- ❑ Reduce On-Hand Inventory
- ❑ Reduce Out-of- Stocks

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

Checkpoint®

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

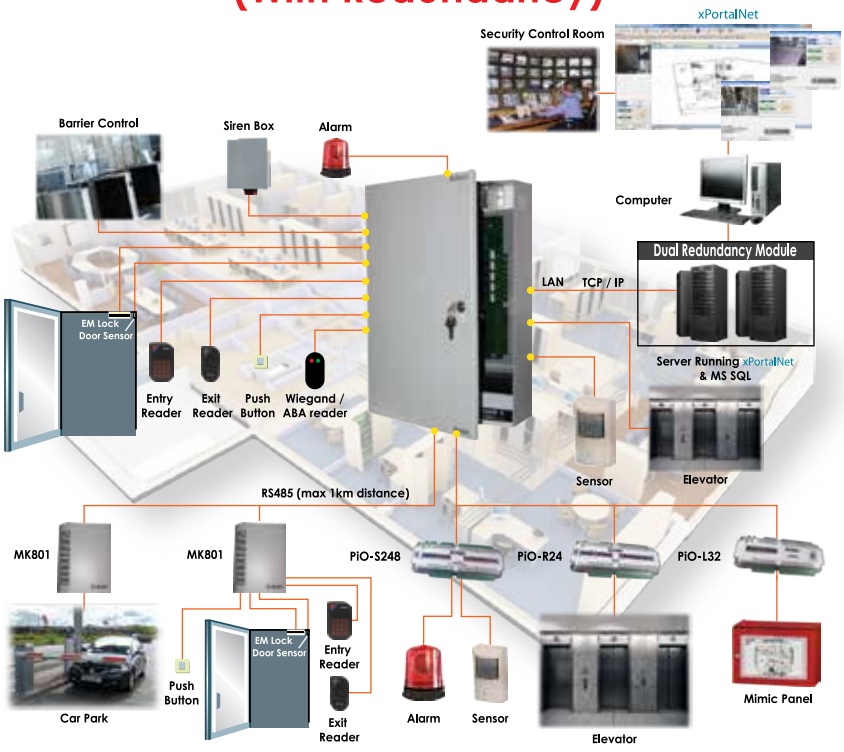
Plato DesFire Reader

- 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

Dear readers of Security Solutions Today,

We have come to the second release of the year for SST – our March/April 2016 issue! I urge you to look forward to interesting stories and articles relating to the healthcare security industry. This issue we will focus on medical care facilities and how the management ensures well-rounded security technologies to guard the safety of their patient, making patient-care a smooth sailing journey.

Case studies are fitted into this March/April 2016 to showcase successful scenarios where security has managed to make the medical arena safe and secured. We join Trend Micro in ways, which the healthcare industry can prepare themselves for upcoming trends of breaches to the systems containing confidential patient information.

For our 'Security Feature', we have Riki Nishimura General Manager of Visual Security Solutions Division, Professional Solutions Company (PSAP) at Sony Electrics Asia Pacific keeping us posted on the Security Demands For Emerging Markets in ASEAN.

The healthcare world is filled with many hidden areas in its system that can easily be hacked into or messed with, if not scrutinised properly. It is a world that needs to be protected of its confidentiality and if compromised, can effect even the public masses who has entrusted a certain healthcare facility. Therefore it is always important for healthcare industries to put their systems in its utmost security.

Putting this issue together has been a wonderful journey and I hope it will be just the same for all of you.

Cheers,

Ain Ebrahim

Only One Company Can Put All The Pieces Together

Fiber Optic Copper Video Data Audio Wireless Ethernet

No Matter What You Need to Transmit, ComNet has Your Solution with the Industry's **Most Complete Line of Transmission Equipment**

› Fiber Optic Audio, Video & Data

› Fiber Optic Ethernet
Managed Ethernet Switches and Media Converters with or without PoE+

› CopperLine® Extenders
Ethernet over UTP/COAX Distance Extenders

› NetWave® Wireless Ethernet
Point-to-Point and Point-to-Multipoint

LIFETIME WARRANTY ∞ MADE IN THE USA WWW.COMNET.NET

ComNet is the Single Source Solution for all your Transmission Products

comnet
Communication Networks

sales-europe@comnet.net
+44 (0)113 307 6400

See what ComNet can do for you.

Secutech India | Stand F3 | 14 – 16 Apr

Smart Cities India | Stand C5 | 11 – 13 May

Dallmeier Presents New IP Cameras With A High Resolution Of Up To 3K High Definition

The cameras of the DF5300HD Topline series have been designed for applications that require high resolution in real-time and simultaneously a good light sensitivity. The most advanced sensor and encoder technology and the sophisticated image processing provide recordings with a resolution of up to 3K High Definition at excellent contrast, brilliant clarity as well as highest detail resolution and colour fidelity.

Very good low-light characteristics

The very good light sensitivity of the sensor and the sophisticated image processing ensure crisp colour images even in low lighting. In night mode, the cameras also provide outstanding results due to the very good infrared sensitivity.

Automatic switching of pre-sets

The cameras are equipped with an ambient light sensor and a removable IR cut filter, and can automatically switch between day and night modes. In addition, different day and night pre-sets for the exposure settings can be defined and adjusted.

Motor-driven varifocal lens

The cameras of the DF5300HD Topline series have a motor-driven megapixel varifocal lens that is perfectly tuned to the image sensor. The adjustment of zoom, focus and iris is made conveniently using a web browser. The manual lens setting directly at the installation site of the camera is not required.

Precise iris control

The P-Iris control provides precise and automatic setting of the optimum aperture. Thus, the cameras achieve a much better depth of field than with conventional DC auto iris lenses under almost any lighting conditions.

EdgeStorage

The cameras are equipped with a RAM memory that is used by the EdgeStorage function for storing the video stream in case of a network failure. When the network is restored, the SmartBackfill function ensures a fast transmission to the SMAVIA recording system. This stores the video stream with high speed and then continues the recording of the live stream seamlessly.

Different housings

The cameras are available with an integrated lens in a compact box housing or in a vandal-resistant dome housing. They can be conventionally supplied with an external power supply unit or conveniently with Power over Ethernet (PoE Class 0, IEEE 802.3af).

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

secutech × solution

19 – 21 April 2016 | Taipei, Taiwan

When **IoT** meets **Security**

Turning tech concept into real business

Catching up with the ever-changing technologies is the key to stand out in the security industry. Growing with the industry trends, secutech – as Asia' largest security solutions show – is here with manufacturing elites who are keen to bring advance technologies such as the internet of things (IoT), Big Data, Cloud services, to **security applications, systems, and solutions** for you to stay on top of the competition!

One Stop Sourcing for Intelligent Security Solutions

Transportation
Industrial
Retail
Building
Smart Home
....many more!

Register Now

www.secutech.com

Delta's Newest EM-Controlled Anti-Terrorist Barrier Provides Less Than Zero Penetration

Delta Scientific of the United States announced that its new HD2055 electromechanically controlled anti-terrorist barricade decisively stopped a 15, 000 pound (6,803 kg) test vehicle traveling at 51 mph (82 kph) in a recent crash test conducted by an independent testing laboratory. The HD2055 barricades not only stopped the vehicle but also contained the test load representing the bombs strapped to the truck bed. The crash test result showed a less than zero penetration.

"Significantly, the operating mechanism and cams were all intact and reusable after the dramatic crash test," emphasises David Dickinson, Senior Vice President of Delta Scientific. "This level of survival is normally only seen with hydraulic barricade systems."

The new HD2055 barricade features an easy-to-install shallow foundation with an environmentally friendly electromechanical actuator, which utilises a sophisticated cam design that accelerates and de-accelerates the barrier road plate during raising and lowering. This reduces the lifting and closing force down to zero at the end of each stroke, dramatically increasing the life of the lifting mechanism.

The shallow foundation also obviates the concerns of interference with buried pipes, power lines and fiber optic communication lines. The HD2055 is perfect for high water table locations and areas with corrosive soils. It provides low maintenance, as all components are accessible from the sides or top of the barrier.

As with its hydraulic designs, the electromechanical HD2055 can be deployed as a single barricade in a narrow lane application or in extended arrays, which cover wide roadways. Each HD2055 barricade can be open or closed individually or as a group to allow the passage of both small and large vehicles.

Like other Delta Scientific products, the HD2055 can be remotely controlled via fiber optics, touch screen control panels; NEMA rated control button panels and simple key switches.

The new HD2055 is available for order now.

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

GJD Launches Its New Website

GJD announced the launch of its new redesigned website: www.gjd.co.uk. The new website has been designed to provide visitors with a user-friendly experience. The site revamp is part of the GJD rebrand and is packed with extensive content as well as a new and intuitive look and feel.

Designed and built with user-experience in mind, the website offers significantly improved navigation and better functionality. It has been complied using the latest technology, ensuring compatibility with all known browsers and devices.

Mark Tibbenham, GJD's Managing Director commented: "We are delighted to announce the launch of our new website. The site and our GJD brand refresh are now more closely aligned with the company's strategic objective for UK and international growth".

continue on page 14

The modern and easy to navigate website offers detailed technical information to help visitors better understand GJD's product range. Useful tools such as product selectors are available to help customers choose exactly which product they require.

Just some of the improvements include downloadable information such as hi-res product and marketing images, as well as free white papers and technical information. Users can also view a variety of installation guide videos and a selection of frequently asked questions on each product category including wired detectors, wireless detectors, lighting control systems and much more.

Visitors can also stay up to date with company news, as well as trends within the detection and illumination industries. The media centre features announcements, latest product innovations and case studies; which provides a detailed overview of GJD's security detection and lighting capabilities across a wide range of sectors.

Ana Maria Sagra-Smith, GJD's Sales and Marketing Director added: "We are very proud of the new website and we hope it provides an informative and useful platform for our customers to get to know our products and GJD better".

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

Xtralis VESDA-E Selected By Telstra To Upgrade Existing And Protect New Switching Exchanges And Data Centres

Xtralis VESDA-E smoke detectors have been selected by Telstra to protect its switching exchanges and data centres against fire threats. Telstra provides 16.7 million retail mobile services, 6.0 million retail fixed voice services, 3.1 million retail fixed data services, and also serves 20 countries outside of Australia. Telstra's critical communication infrastructure has been protected by VESDA solutions for decades, with VESDA Xenon and Laser-based detectors deployed since the late 1990's. With VESDA-E VEU, Telstra is matching its state-of-the-art communications facilities with the best in very early & reliable smoke detection and fire protection, ensuring its customers have the complete reliability and service continuity.

Only VESDA can provide the sensitivity & reliability to ensure smoke & fire threats are prevented in telecommunication and data communication facilities and Telstra's long use of VESDA is a testament to that. As data and information service needs grow, Telstra is both retro-fitting existing facilities and expanding with new facilities, and VESDA-E VEU will be the smoke detection system to provide reliable threat prevention for both. The ease of integration and backward compatibility with existing Xenon and Laser products provided an additional benefit to Telstra.

"We're proud to serve Telstra with the new VESDA-E VEU systems, as we have worked with them for many years," commented Eddie Tieppo, Xtralis Sales Director for Australia, New Zealand and India. "Telstra is a world-class organisation, and they recognized the value of VESDA early on. Our systems have protected their facilities for many years. With VESDA-E VEU we expect to protect Telstra's critical infrastructure for many years to come. It's an honour to protect the best with the best," said Tieppo.

VESDA-E is the latest-generation of VESDA aspirating smoke detectors, featuring multiple innovative capabilities that dramatically improve the VESDA experience, including increased sensitivity, up to 8 per cent less power consumption per unit area, future proof expandability and programming, analytics to provide unique particle type characterisation capabilities, and extensive connectivity options — all while reducing the total cost of ownership (TCO) for the world's best smoke detection. Built with patented Flair technology, VESDA-E represents a significant evolution of the popular and widely deployed VESDA Xenon and VESDA Laser series. VESDA-E is the perfect fit for upgrading aging technology as it is fully backward compatible and offers an enhanced user experience, wider connectivity options, and analytics for effective and efficient response.

For more information, please visit: http://www.xtralis.com/Upgrade2VESDA-E SST

Milestone Systems Celebrates MEA Focus At Intersec 2016

Milestone Systems showcased the award-winning XProtect portfolio at their crowded stand at Intersec 2016, held in Dubai last week.

The official launch of XProtect 2016 took place at Intersec signaling the importance of the Middle East Africa (MEA) region to Milestone. The software was unveiled with enthusiastic response as the new version of the market-leading software has numerous enhancements to put Milestone customers and partners in more control than ever before.

A full range of camera partners and solution partners presented at the Milestone booth, showcasing the continuing power of open platform technology and the expanding partner community. This led to the most successful Intersec event ever for Milestone and its partners.

The partner response was very positive:

"Participating in the Milestone stand at the 2016 Intersec Expo in Dubai was an amazing experience. As a member of the Milestone Open Platform Community, ISONAS was able to actively participate in educating customers on the new XProtect 2016 product, open their eyes to possibilities in integration to access control, and in turn refer them to additional technology from other partners in the same stand," said Robert Lydic, Global VP of Sales, Isonas. "The customers were delighted, and as a participating vendor partner, I was extremely pleased with the interaction with the Milestone EMEA team."

Regional expansions

Milestone has been growing rapidly in the region over recent years, and the MEA team expanded by 35 per cent in 2015. Three new Milestone offices have been opened in Beirut, Jeddah and Johannesburg. The success for Milestone MEA has risen by more than 30 per cent, as the area embraces the Milestone partner-driven business model, which ensures customers a local presence with a global connection.

"Our declared aim for the future is to strengthen our local footprint: we are honored to be chosen by so many highly esteemed customers here. We will build on this positive response to further leverage our dedicated partner community using the open platform strategy toward our joint customers' advantage," said Peter Biltsted, Sales Director, Middle East & Africa, Milestone Systems. "It was a very successful Intersec 2016 for our partners and us. In particular, the huge interest shown by visitors who came from the entire MEA region, is a clear indication that the market is accelerating."

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

Toshiba's IK-WB82A Sets Higher Standard For Bullet-Style IP Video Surveillance Cameras

Bullet cameras are noteworthy for their slim, easy to install profile and cost-effective deployment in IP video surveillance systems. Toshiba Surveillance & IP Video Products, a business unit of Toshiba America Information Systems, Inc., today set a higher standard for this camera category by introducing its new IK-WB82A. This bullet IP camera features three-megapixel resolution (2048 x 1536), adaptive IR LEDs and H.264 Smart Codec high-compression technology that reduces network bandwidth and storage requirements compared to standard H.264 compression.

"The IK-WB82A puts high resolution, bandwidth efficiency, and ease-of-use in the hands of security professionals who need a bullet camera indoors or outdoors, especially in environments that present complex, challenging lighting conditions," said Greg Hartzel, Director of Toshiba Surveillance & IP Video Products. "Outdoor city surveillance, railway platforms and retail stores would all benefit from the camera's superior combination of performance and value."

The camera's launch comes as concerns have grown over the burden of placing high-resolution streaming IP video on already overloaded networks and storage devices. Smart Codec addresses the bandwidth issue by effectively reducing a video packet size. The key to Smart Codec's success is that it allocates more bandwidth to moving objects or critical areas of interest, and less to background images.

Despite many advances in IP camera technology, capturing video in low or extremely bright lighting remains a challenge. To overcome it, the IK-WB82A incorporates features such as Adaptive IR™ automatically adjusts the IR LED intensity in order to avoid over-exposure of close objects, True Day-Night Imaging, and True Wide Dynamic Range to handle high-contrast scenes where sunlight makes areas that are bright and others with dark shadows. IR illumination range is an impressive 30 meters.

Because every area that needs to be monitored is not a perfect square the IK-WB82A has a user-controllable "Hallway View" that rotates the camera view 90 degrees to effectively create a "portrait" mode. Security professionals tasked with monitoring long narrow spaces such as retail aisles, hallways, office corridors and stairways will greatly appreciate this viewing versatility.

The ruggedly built IK-WB82A is rated IP66 for use outdoors. It is also ONVIF complaint for seamless integration with third party equipment.

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

S2 Security Introduces S2 MicroNode Plus

S2 Security introduced S2 MicroNode Plus, the company's latest two-reader panel for S2 NetBox series web-based access control and event monitoring systems. New product features include a Power over Ethernet Plus (PoE+) power option, storage for up to 150,000 cardholder credentials, and faster processing.

"S2 Security routinely updates its hardware products to reflect compelling new technology," said John L. Moss, CEO, S2 Security. "S2 MicroNode Plus, with its more powerful processor, expanded credential memory, and increased PoE

continue on page 17

capacity is an excellent example of this."

S2 MicroNode Plus supports up to two portals, four relay outputs with wet/dry selection, four inputs with programmable levels of supervision, and one temperature input. In addition, the appliance includes a 12VDC auxiliary output for powering devices such as a PIR Request to Exit input or an alarm sounder. Access control and events from connected devices are aggregated to the S2 NetBox web interface for centralised system management.

S2 MicroNode Plus is also an ideal retrofit solution. The seamless upgrade from legacy two-reader panels can be made without replacing readers, inputs or lock outputs.

For more information, please visit: www.s2sys.com SST

Dahua Technology Introduces Smart Thermal Network Camera Series

Dahua Technology introduces the smart camera series to provide superior image quality and advanced features for perimeter, electric industry, manufacture security applications. The camera series is designed to find heat sources, able to offer highly detailed images and an extensive feature set.

Dahua's new smart thermal network camera family includes thermal hybrid PTZ camera, hybrid speed dome camera, thermal bullet camera and thermal dome camera, all equipped with a variety of smart functions. The smart thermal cameras adopt top-notch sensor that is capable of detecting tiny differences in temperature. Those camera series can achieve higher detection accuracy and it is able to function in complete darkness and adverse weather conditions. Furthermore, the cameras consist of combined intelligence, efficiency and high performance such as smart detection, smart analysis, smart perception, smart tracking and smart control.

The smart thermal network cameras can determine the object's precise temperature and the temperature distribution even on small and fast-moving objects. Those cameras are excellent for detecting water leak behind a wall, a person hidden in the bushes at night, or identify passengers with a fever passing through a checkpoint.

Dahua also provides software and accessories include smart PSS, NVR and DMSS to work together to meet the individual requirements of transportation industry, energy industry, border and coastal surveillance, etc and other special applications.

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

Evolis Wins Industry Accolades For Outstanding Business Performances

The 2015 Growth Champion Award

The Actionaria Trade Fair held on November 20 and 21, 2015, at the Palais des Congrès in Paris, welcomed the FUTUR40 Awards organised by the magazine "Croissance Plus" and the "PME Finance" business association.

These coveted awards honour SMEs and midmarket companies listed on the Paris stock market that have a proven track record of dynamic growth over the past three years. Evolis was recognised as a 2015 growth champion along with 40 other companies.

The Jury's Favourite Special Award For Leading SMEs And Midmarket Companies

The MOCI trade magazine recently announced its 7th Annual National Ranking of leading SMEs and midmarket companies operating internationally, with Evolis topping the ranks of the Jury's Favourite Special Award.

This prize, which is awarded to 10 companies, is based on the annual ranking of the 1,000 leading SMEs and midmarket French companies operating at a global scale. This award recognises the success of Evolis' international development strategy and products.

The award ceremony took place on November 27, 2015 at the Chamber of Commerce and Industry of Paris, in the presence of Matthias Fekl, the French Secretary of State for Foreign Trade.

As Emmanuel Picot, CEO, Evolis, points out "these awards recognize the relevance of our development strategy and the expertise of our teams to achieve such premium business performances. Our production facilities have been optimised; our organisational structure has been revamped; and our significant diversification has helped expand our range of solutions. We are therefore poised for further dynamic growth, especially in the international market."

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

Trend Micro And ASUS Partner To Deliver A New Level Of Smart Home Security

According to Business Insider, Internet of Everything (IoE) home devices will reach 20 billion by 2019, and will soon face critical security issues. Trend Micro Incorporated announced that it has expanded the partnership with ASUS for the new ASUS Smart Home Gateway, which will come equipped with a Trend Micro security development kit (SDK), designed to establish safe connections between smart devices, apps, and cloud services. The two companies have collaborated last year to create the Trend Micro Smart Home Network solution wireless routers.

"As IoE becomes ubiquitous, the chances of connected devices, such as IP cameras, smart lighting, and refrigerators, getting hacked will increase as well. Should there be no security in place, personal privacy and safety will be at risk. With this in mind, Trend Micro developers have committed thoroughly to enhancing in-house security to defend against advanced threats. We are excited to collaborate with ASUS once again to integrate the Trend Micro SDK and ASUS Smart Home Gateway. This solution will filter and intercept malicious intrusions and attacks to protect the entire home network. We hope our partnership will set an example for more vendors to emphasise IoT security for homeowners. We'd be most keen to partner with more hardware makers to provide more custom smart home solutions that deliver comprehensive protection for the connected home environment," stated Steven Hsu, Director of Global Consumer Sales Enablement & Business Development at Trend Micro.

"Trend Micro has long been developing the most advanced security protection technologies," says Jim Yeh, Senior Director, Smart Home Department at ASUS. "We are elated to once again work with them to bring our security solutions to the next level. By embedding the Trend Micro SDK within the ASUS Smart Home Gateway, this development offers well-rounded security features for energy-saving homes."

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

VIVOTEK Ensures Both Safety And Security At Iran Chaponashr Printing And Publishing Factory

VIVOTEK's IP surveillance solutions have been successfully applied by an innovative printing and publishing firm located in Tehran, Iran called Chaponashr Printing and Publishing Factory. To best monitor the movement of materials, visitors and employees throughout the facility, Chaponashr enlisted the expertise and experience of Pooya Fara Negar (PFN) Technology to deploy VIVOTEK's comprehensive and reliable IP solutions to fulfil a range of surveillance demands. As such, 9 different VIVOTEK camera models were used, and a total of 171 cameras were installed at Chaponashr's facility, all connected to 2 network video recorders (NVRs) and controlled via VIVOTEK's own VAST software.

Within Chaponashr's production and binding saloon, as well as the facility's main entrance, 4 2-megapixel SD8363E speed dome network cameras were chosen for their 360-degree monitoring capability and 20x zoom function, allowing comprehensive monitoring and optimal image delivery of the facility's surroundings.

A further 92 2-megapixel IB8369 bullet network cameras were installed throughout the facility. These cameras provide a great cost-to-benefit ratio with a range of features including built-in IR illuminators effective up to 20 metres and weather proof IP66-rated housing.

Adding another layer of security, 11 units of FD8137H and FD8169 were installed throughout Chaponashr's well-lit office space, making use of the two models' ability to handle natural or bright-light conditions thanks to WDR functionality. Finally, all of these extremely capable network

cameras are connected to two NVRs via VIVOTEK's VAST software with 200 licenses, allowing security footage to be recorded and monitored in real-time from a centralised, secure location within Chaponashr's facility.

Alex Kuo, Department manager of VIVOTEK's International sales department I, is excited about the project, saying "thanks to the cooperation of these two innovative, forward-thinking firms, VIVOTEK once again has provided a high-tech, comprehensive monitoring solution to a company with a once difficult, but now superbly solved, security-monitoring dilemma. Chaponashr, Pooya Fara Negar (PFN) and VIVOTEK will continue to innovative and move forward in the 21st century within respective industries, and consumers and clients alike will continue to benefit from our advancements."

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

Surveon New Premium VA Camera Series Optimises Business Operations

Surveon introduces three new 3-megapixel VA cameras, CAM2441HI, CAM3471HI, and CAM4471HI for its premium series. Featured with the intelligent video analytic functionality, the new models deliver advanced applications, including motion detection, camera tampering detection, and people/object counting to provide historical, current and predictive views of business operations and help users to make optimal use of their surveillance systems and allocate their time and attention in a more effective manner, thus increasing the return on investment in the surveillance system, as well as improving overall security, safety and profitability.

"These days, a massive amount video is being recorded, but never watched or reviewed. As a result, events and activities are missed, and suspicious behavior is not noticed in time to prevent incidents," said Casper Wu, product manager of Surveon. With the intelligent video analytic functionality, Surveon's 3 megapixel VA camera series can transform raw data into meaningful and useful information for business analysis purposes and to easily upgrade to advanced surveillance to have loss prevented, profitability improved, shrinkage reduced, better services brought to customers and thus true business operations can be optimised.

In addition, this series offers 2048x1536 resolutions at 30FPS and Smart Auto HDR with 120dB, giving users' real-time performance and outstanding video visibility even in very low lux or highly complex lighting conditions. Along with other advanced functions such as the smart IR, smart shutter, P-Iris, and enhanced 2D/3D noise reduction, Surveon provides intelligent surveillance solutions for mission-critical applications such as retail, banking, transportation, public utilities and city surveillance.

CAM2441HI

CAM3471HI

CAM4471HI

The new models come in three different form factors, including box (CAM2441HI), outdoor bullet (CAM3471HI), and outdoor dome (CAM4471HI), for a variety of deployments. Its numerous features make the series easily stand out in the massive selections of IP cameras and offer the advanced technology, and competitive edges for partners. All Surveon's megapixel cameras support the ONVIF standards and are fully compatible with Surveon VMS and the major third party VMS, giving partners a broad range of solution selections for their projects.

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

Security Trends In The Healthcare Industry

- New Risks And Priorities For Keeping Patient Information Safe

Article by
Michelle Alvarez
Threat Researcher and Editor, IBM Managed Security Services

Contributors
- **Pamela P Cobb**, Market Segment Manager, X-Force and Threat Portfolio, IBM Security Systems
- **Jason Kravitz**, Techline Specialist for IBM Security
- **Marcelle P. Drakes**, Security Services Specialist

Introduction

The healthcare industry used to be on the sidelines of the cyber war, with breaches and malicious attacks far more common elsewhere. That has changed. Five of the eight largest healthcare security breaches over the last five years — those with more than 1 million records compromised — happened during the first six months of 2015. Almost 100 million healthcare records were compromised. The cost of those breaches is likely to be enormous. In most cases the costs will probably be also considerably higher than those of similar breaches in other, unregulated industries. As the Ponemon Institute's 2015 Cost of Data Breach Study found, a healthcare record lost or stolen in a breach could cost the victim organisation as much as $363, fully 136 per cent higher than the global average cost of a data breach per lost or stolen record.

The healthcare industry is a popular target because Protected Health Information (PHI) has an excellent resale value on the black market. So is Electronic Health Records (EHRs) that can contain a patient's email, social security number and banking and employment information, as well as health and medical data.

The consequences of compromised PHI are many. As well as the costs an organisation suffers, its customers too can face all kinds of potential expense and hardship. For one thing, stolen data cannot be re-privatised once it has

been disclosed; unlike a stolen credit card that can be easily replaced, an individual's healthcare history cannot be erased and swapped for a new one.

The prospect of high financial gain is one factor drawing attackers to the healthcare sector; the other one is the numerous attacks of vectors the industry offers through its widespread use of legacy systems and dated technology, allowing tried-and-true attack methods. Social engineering via spear phishing and other scams are proving successful. And the cloud, mobile apps, and the Internet of Things are growing industry trends that expand the attack surface for new exploitation vectors.

Daunting, as these security challenges may seem, healthcare organisations willing to put cybersecurity at the forefront of their priorities are in a strong position to prevent attacks and compromise.

The year of the healthcare security breach

Four years ago, in the midst of frequent reports of data leaks, denial-of-service attacks and social hacktivism, IBM X-Force declared 2011 the "Year of the Security Breach." Today, with close to a hundred million healthcare records compromised in the first half of the year, 2015 so far looks very much like the "Year of the Healthcare Security Breach" (see Figure 1).

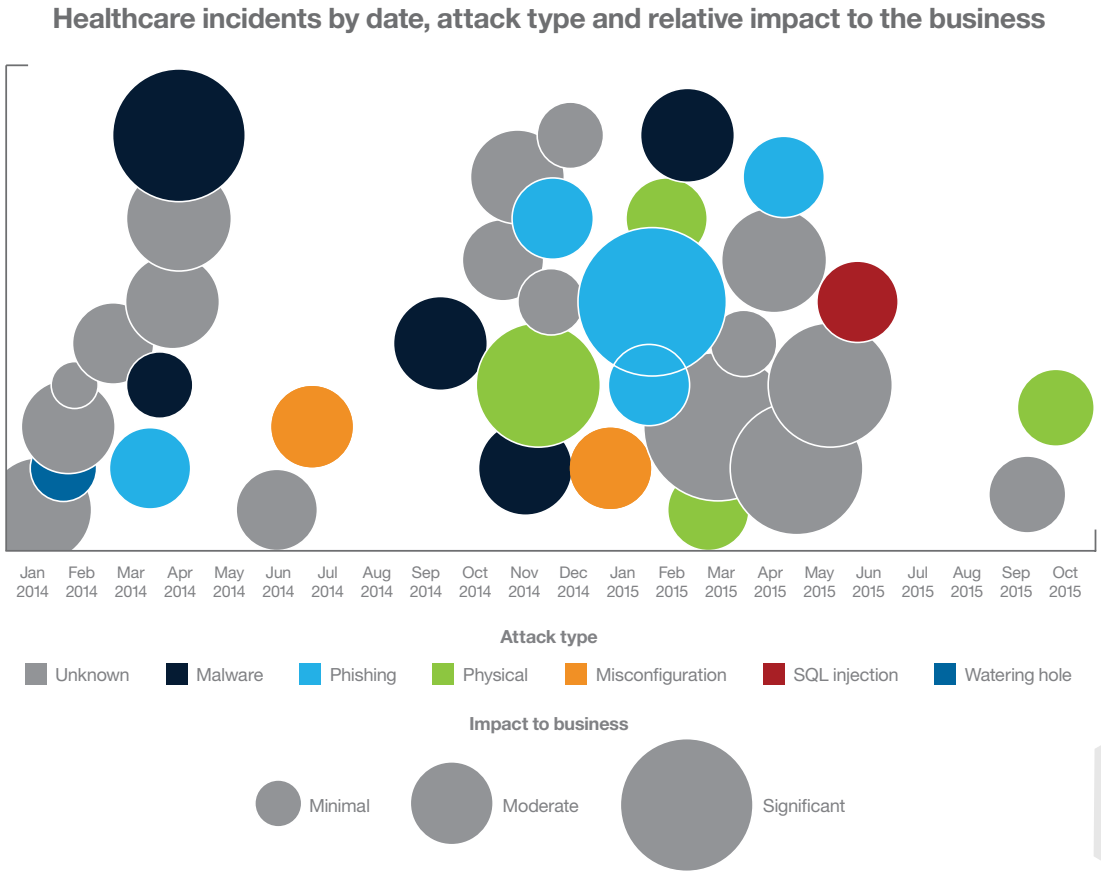


Figure 1. Healthcare security incident timeline. Source: IBM X-Force Interactive Security Incidents data (January 1 2014 – October 31 2015). Note: Data is a sampling of notable incidents and not a full representation of all incidents.

Nearly 100 million records compromised in 2015

Based on information IBM X-Force gathered about notable security incidents in the first 10 months of 2015, healthcare ranked #1 in terms of records compromised, with nearly 34 percent of all records compromised across all industries (see Figure 2). Considering that between January 2011 and December 2014 the industry accounted for only .63 percent of total records compromised, that's a significant climb. The five very large security breaches mentioned earlier contributed significantly to this rise in ranking. PHI data fields from those breaches included emails, social security numbers, banking and employment information and medical records. Interestingly, healthcare has hung on to its #1 ranking even though the second half of 2015 has yet to see the same level of large-scale breaches affecting the healthcare industry as seen in the first half.

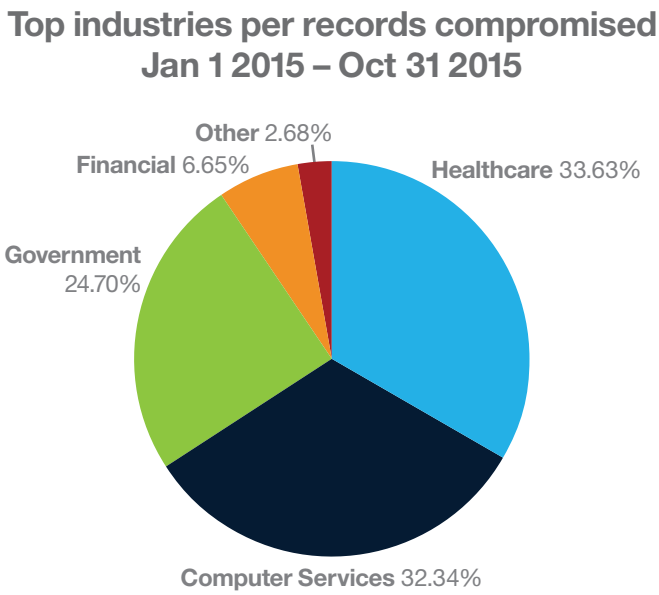


Figure 2. The healthcare industry holds first place by a small margin over computer services in terms of records compromised in the first ten months of 2015. Source: IBM X-Force Interactive Security Incidents data (January 1st 2015 – October 31st 2015). Note: Data is a sampling of notable incidents and not a full representation of all incidents.

According to the healthcare organisation that suffered the largest breach yet publicly reported, the compromise was due to a "very sophisticated external cyber attack." The same is suspected of being true in another massive breach of a healthcare institution. Both incidents clearly demonstrate the dangers posed to healthcare by external adversaries.

Such threats are a significant concern, particularly when they emanate from outside an organisation's home country. Yet, the threat from inside should never be overlooked. As the IBM 2015 Cyber Security Intelligence Index states, "55 per cent of attacks [for all industries] were carried out by those who had insider access to organisations' systems." That number includes both malicious insider and inadvertent actor attacks, the latter defined as an attack or suspicious activity allegedly executed without the user's knowledge from an IP address inside the organisation's network.

Most such users are employees, but they can also be trusted third parties — partners, clients, maintenance contractors — with whom an organisation conducts business. In fact, one of the largest healthcare breaches of the last five years was the compromise of a provider of software services to the healthcare industry.

Nearly 50 per cent of healthcare breaches have an undisclosed attack type

In almost half of the healthcare breaches sampled, the victim organisation has not to date disclosed exactly what type of attack they sustained (see Figure 3). This may be because they did not know at the time the breach went public, or they were in the process of investigation. When the attack type is not revealed, the public may raise important questions about security posture and handling of the attack. Was a cybersecurity incident response plan in place? Was an emergency response services team engaged? Were there comprehensive auditing capabilities for at least the critical systems, particularly those containing electronic PHI?

In another scenario, perhaps the breach was still under investigation and the victim planned to disclose the findings later. Then again, the healthcare organisation might have decided against public disclosure because it feared copycat attacks or believed that the information wasn't relevant to the public. From the security researcher's point of view, that's an unfortunate way to approach breach disclosure, because sharing experiences and indicators of attack can be critical to the task of strengthening everyone's cyber threat defenses. Knowing how other organisations in an industry are being attacked helps security professionals determine where risk must be addressed, which in turn helps everyone spend security dollars more effectively.

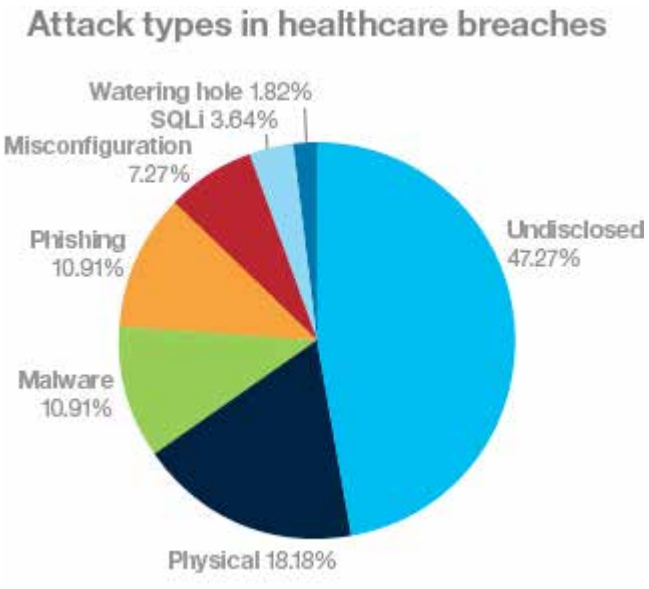


Figure 3. "Physical" ranks second as most prevalent attack type affecting the healthcare industry. Source: IBM X-Force Security Incidents data (January 1 2011 – October 31 2015). Note: Data is a sampling of notable incidents for each year and not a full representation of all incidents.

Insider threat: a growing concern for healthcare

Of the attack types disclosed, the "physical" category ranks highest (see Figure 3). Physical attacks run the gamut from someone stealing an unencrypted laptop out of an employee's car to employees with privileged access selling PHI on the black market. The latter is considered a malicious insider attack An insider is anyone who has physical, logical or remote access to a company's assets: information in transit (data moving through the network via email, web or other Internet protocols) or tangible items such as hard-copy documents, disks, electronic files, laptops and the like.

There are several actor profiles within this category: the disgruntled employee, the malicious insider seeking financial gain, the quasi-insider considered a trusted third party, and the inadvertent actor who falls prey to social engineering schemes, granting access to an outside attacker. With phishing and malware accounting for nearly 24 per cent of disclosed attacks, the impact of social engineering and the inadvertent actor on the healthcare threat landscape is clearly significant.

Prevalent attacks targeting the healthcare industry

IBM Managed Security Services (MSS) continuously monitors billions of events reported every year by thousands of client devices in over 100 countries. Analysis of the data accumulated between January 1, 2014, and October 31, 2015, reveals some interesting findings about attacks against the healthcare industry.

Malicious documents and sites

Fooling victims into opening malicious documents or clicking on links to malicious sites are proving to be very successful attack methods in the healthcare industry, with the document angle appearing preferable to the link approach. 33 per cent of the attacks involved these techniques, with almost 5 per cent of this total involving attacks exploiting file image and media player vulnerabilities. As we explain below, spear phishing increases the effectiveness of these attacks.

Shellshock

One of the threat game changers for 2014, Shellshock is the number two attack vector, making up just over 16 percent of the attacks. Shellshock is vulnerability in the GNU Bash shell widely used on Linux, Solaris and Mac OS systems and is well documented by the IBM 2015 Cyber Security Intelligence Index. This "malware-less" attack vector remains a significant and persistent threat across all industries in 2015, not just healthcare. Attackers are looking to exploit existing functionality in applications rather than risking malware detection that would thwart their success.

Brute force attacks

A brute force attack, the number three vector at just over 10 percent, uses an automated, repetitive method of trial and error to guess an individual's user name, password, credit card number or cryptographic key. This type of attack has been prevalent across other industries in addition to healthcare. The IBM report The price of loyalty programs highlights an upward trend in brute force attacks targeting account passwords.

Successful exploitation could allow an attacker to access user profile data or confidential documents stored on the web application or server. Hackers who gain access to an administrator account can inject malware that turns websites into distributed denial of service (DDoS) bots, or they can deface or disable a company's website and distribute malware that might lead to blacklisting on Google and other search engines.

Honorable mention: older and non-sanctioned applications

IBM MSS found many attempts to exploit a vulnerability affecting VBScript. This active scripting language is not supported in Internet Explorer 11. Healthcare organisations running earlier versions of Internet Explorer are at risk of attackers using VBScript to execute arbitrary code on a vulnerable system. We address the use of legacy applications more fully later in this report.

Like older applications, non-sanctioned applications can present a problem. IBM MSS found that healthcare industry employees use a number of applications, from file sharing apps such as Dropbox to apps like TeamViewer that facilitate online meetings, which may or may not be officially sanctioned by the organisation. Bringing end user devices into the security fold can be difficult, presenting attackers with an additional attack vector.

A playground for scammers and spear phishers

Attackers today get a much bigger black market bang for the buck—or bitcoin—when their merchandise is medical records, not "plain old credit card data." It has been reported that an electronic health record can bring 50 dollars versus typically a few quarters or dollars for a credit card number. Why? What's in a medical record that makes it so appealing to scammers, spear phishers and other cyber criminals?

Credit card data is an ingredient, but there can also be email addresses, social security numbers, employment information and medical history records. That information opens victims to spear phishing campaigns and can be used against them in all kinds of ways: sabotaging their jobs, ruining their credit, and destroying their public image or professional reputation.

Included within "medical history" is another asset attackers can leverage: medical images. IBM researchers estimate that medical images are by far the largest, fastest-growing data source in the healthcare industry, accounting for at least 90 per cent of all medical data today. Criminals can combine the knowledge gleaned from these images with the other data they find in medical records to custom-tailor their scams or attacks.

A victim whose images show rheumatoid arthritis, for example, could be targeted with a tailored email campaign for pain relief and persuaded to click on a link to a fictitious pain management site, thus downloading malicious code. Since many EHRs include financial and employment information, sifting through data to find suitable victims for a fraudulent health plan or discount medical card can be a simple job for a scammer.

Medical records are also highly prized for use in medical identity theft, a crime on the rise. According to the Ponemon Institute's Fifth Annual Study on Medical Identity Theft released in February 2015, medical identity theft incidents increased 21.7 per cent since last year's study. Thieves use stolen identities to access medical treatment, to acquire prescription drugs for sale or personal consumption, and to make false claims against the victim's health insurer through fraudulent clinics.

Like the identity thief, the spear phisher mines the rich vein of data buried in health records for easy money — and the more data acquired, the sharper the spear (or social-engineering hook) in a spear-phishing email. As we saw in the Dyre Wolf campaign, an attack targeted at the banking industry, which resulted in millions lost by targeted organisations, some of the most elaborate, sophisticated multi-step attacks begin with an appropriately calculated spear-phishing email.

Transforming business and introducing risk

Technology has helped the healthcare industry make great strides in the advancement of care, but it can also pose increased security risk.

Internet of Things can open more doors for attack

The Internet of Things (IoT), and more importantly the insecurity of all the devices or "things" it encompasses, is the focus of many enterprises today. That is because the sheer number of devices is going to grow exponentially. Gartner, Inc. forecasts that 4.9 billion connected things will be in use in 2015, up 30 per cent from 2014, and will reach 25 billion by 2020. Although manufacturing, utilities and transportation are the major IoT industries at play, healthcare is also in the game. One research firm predicts that by 2020 the healthcare IoT market segment will reach $117 billion.

Why is the proliferation of IoT a security concern in the healthcare industry? A review of some of the medical devices used in hospitals, homes or both—surgical and anesthesia devices, ventilators, drug infusion pumps, external defibrillators, patient monitors, and laboratory and analysis equipment, to name just a few—paints a troubling picture. Over the last few years, researchers have been uncovering vulnerabilities in these devices, many of which play a vital role in supporting or sustaining life. In 2013, the Industrial Control Systems Cyber Emergency Response Team, or ICS-CERT, released an alert warning of a hard-coded password vulnerability affecting about 300 medical devices across approximately 40 vendors — in terms of sheer numbers, a huge discovery.

Some more recently disclosed medical device vulnerabilities are being targeted by publicly available exploits, and some could be exploited by "an attacker with low skill." Another recent ICS-CERT report disclosed that a remote attacker could gain control of an intravenous pump used in the US and Canada. Remote attackers might modify critical settings or device firmware, and disturbing real-world scenarios could ensue: drug pumps reprogrammed to deliver incorrect dosages, defibrillators disabled. Finding connected medical devices to target is as easy as visiting Shodan, a well-known search engine that allows users to locate Internet-connected devices.

Attackers might want to exploit devices to cause injury or death, which is an obvious and serious concern. Another scenario is security compromise for financial gain (i.e., extortion). A recent IBM MSS report highlighted a popular method of extortion, distributed denial of service (DDoS) attacks. Attackers are known to diversify their targets and could very well threaten to apply the DDoS extortion attack vector to medical devices. Extortionists might first demonstrate their capabilities by slightly altering a device's functionality, then follow up with an email demanding that the victim pay up within a certain time limit or face graver consequences—a denial of service of the targeted medical device.

Theft of data via devices is also a risk. A report earlier this year on a vulnerability in several medical devices that was used to steal data from a hospital's databases suggests the possibility that we are seeing just the tip of the iceberg. One can wonder if the healthcare industry has this potential problem in their sights. It could be that with device manufacturers focusing on potentially life-threatening issues evident in the staggering number of reports of "suspected device-associated deaths, serious injuries and malfunctions" received every year by the U.S. Food and Drug Administration, device manufacturers do not yet regard the resolution of vulnerabilities resulting in information disclosure as a top priority.

Mobile health apps: another gateway to exploitation

A 2013 study found there were 97,000 mobile health applications in major app stores, a staggering number that one would expect to be even larger by now. Quite apart from controversy about whether health apps can be unreliable or even dangerous, there can be serious security risks associated

with mobile apps in general. For example, earlier this year researchers disclosed a flaw in the way thousands of popular mobile applications, including medical apps, store data online, rendering the applications exploitable by attackers. It is clear that mobile applications in the hands of both consumers and medical staff can be attack entry points.

Security in the cloud

IoT and mobile apps aren't the only developments transforming the healthcare industry. A growing number of healthcare organisations are using software as a service (SaaS) in the cloud to host applications and data and to improve costs and efficiency. Health information exchange (HIE) systems that allow for the mobility of healthcare information electronically across distinct systems are increasingly cloud-based.

Federal and state incentive programs in the US encourage the use of HIEs, but some healthcare organizations have been reluctant to move towards a cloud-based system because not all cloud services vendors offer HIPAA business associate agreements. Organisations should recognise that selection of a cloud service provider is an important decision that should be based on close scrutiny of the service provider's commitments and statements regarding compliance with HIPAA.

Legacy systems and processes, lack of funding

As we've noted already, IBM MSS found that many healthcare industry organisations' IT systems were exploitable via an older Internet Explorer VBScript vulnerability. The web browser is a popular attack vector, but not the only one. According to one source, as of September 2015, Microsoft Windows XP holds over 12 percent of the installed operating systems for desktops, yet Microsoft ended technical support and security updates for Windows XP operating system on April 8 2014. That 12 per cent is dispersed across many industries, but it includes the healthcare sector—leaving vulnerable systems open to exploitation.

Migration to newer versions of an operating system or web browser requires time and money, and a lack of funding may be one of the fundamental obstacles to improving the security posture of the healthcare sector. As a survey released last year by the Healthcare Information and Management Systems Society reported, nearly half of the responding healthcare organizations spend three percent or less of their IT budget on security. The percentage may be slightly higher on average today.

This may not seem sufficient to cover what might be required—i.e., replacement of expensive equipment. A recent report highlights that the ideal spend on security is 13.7 percent of the overall IT budget, while a survey from 2014 indicates US firms are spending as much as 15 percent of their IT budgets on security. Even with adequate funds, some organisations are unable to migrate off of legacy platforms because their equipment is incompatible with newer versions of Windows, or drivers for newer versions of Windows are not available for expensive equipment such as CT and MRI machines.

Unfortunately, legacy operating systems and dated applications are only one facet of a many-sided dilemma. Healthcare companies may still use heritage processes without updating security practices around them. Many organisations, even those that have adopted electronic health records, are still keeping some form of paper records. Bags full of private, confidential medical documents are still being found in trash bins — a perfect example of a route to security compromise. (In addition, failure to implement reasonable safeguards to protect PHI when disposing of medical records violates HIPAA rules and could result in fines and penalties.)

When the organization is keeping electronic health records, is the PHI encrypted? There's a chance it isn't. Under HIPAA, each institution is free to assess risk to its electronic PHI and decide for itself

whether encryption is or is not reasonable and appropriate. There is ample room for interpretation, and it's conceivable that organisations may not always make the decision to encrypt.

One of every organisation's major challenges is how to address cyber risk in order to direct IT investment and resources most effectively. Healthcare organisations may feel the pressure of this issue more acutely than those in other sectors because of the sensitivity, volume and velocity of the data traveling through their networks. The fact that attackers can see them as a rich environment for stealing data and threatening harm of immediate physical or financial consequence speaks volumes for the pressing need for healthcare organisations to assess risk, address issues and focus investment.

Where should limited funds be focused?

Healthcare organisations that have placed someone in charge of security strategy, worked out an incident response plan, and made wise choices about data protection policies will fare better when they face a potential breach or compromise.

Who is running the show?

Security problems left unmanaged will take root and run amok, so they must be managed, and someone has to be in charge. In large organisations, that person should be a full-time Chief Information Security Officer (CISO) who can help steer the overall security strategy and budget. CISOs answer the burning question: Is the organisation making the right calls on security-related solutions? They understand the company's assets and the threats to which those assets are most susceptible. Moreover, they have the status to present important security matters to the organisation's board of directors and affect needed changes. Smaller organisations may not require a CISO, but they should still have a dedicated information security person with the power to make risk-benefit decisions that improve the overall security posture of the organisation. In fact, HIPAA mandates the designation of a security official "responsible for developing and implementing its security policies and procedures."

Get ready now

Waiting for a hurricane to make landfall before you get bottled water and batteries is not the best course of action. The roads may be unsafe and the supermarkets closed. It's the same when the looming threat is a cyber incident. In both scenarios, what you need most of all is preparedness. Specifically, the cyber threat to your organization calls for an incident response plan, or IRP, that helps you comply with HIPAA and other regulations. Plus it can change your security stance from reactive to proactive, potentially saving you a great deal of time and money. Your IRP should be a dynamic document reviewed regularly, with changes made wherever they are needed following an incident.

But well-documented procedures go only so far. Every organization must also have staff capable of carrying out the IRP and calming the chaos of a security incident. Only a team well versed in the response program can deliver the consistency and efficiency needed to streamline responsiveness. Above all, the team must be well trained.

Review medical devices for security issues

Securing medical devices can be an uphill battle for hospitals. Some service-level agreements between the device vendor and the healthcare facility dictate that the vendor is responsible for patching the device, some further stipulating that it be patched at the manufacturer's facility. Moreover, many devices also require a skill set the hospital IT staff might not possess. All these factors can make performing device security updates an arduous undertaking for all involved.

There is no substitute for security updates and they should be performed. In addition, other steps can be taken to help protect against the use of medical devices as an attack vector:

- Test and evaluate devices before deploying them. Report potential security issues to the manufacturer or the FDA.
- Restrict unauthorized access to networked devices.
- Ensure that firewalls are up to date and perform periodic configuration reviews.
- Monitor network activity for unauthorised use.
- Perform audits of the devices; collect logs and review them regularly.
- Perform penetration testing of medical equipment, including implantable medical devices.

Other essential data protection methods

Encryption. Encryption. Encryption. Passwords should be encrypted, especially those for privileged users. Wherever possible, you should:

- Encrypt patient information, even at rest and within the EHR.
- Segregate patient data from other data and use different subnets.
- Follow the principle of least privilege, allowing data access only to users who require it to do their jobs.
- Implement defense in depth with multiple layers of security.

Bear in mind that while encryption is certainly a key component, it's only one aspect of a strong identity and access management program that every healthcare firm should implement.

Make cyber security a business priority

A survey released earlier this year found that about 80 percent of healthcare organisations surveyed were confident they would pass a random HIPAA compliance audit. That's good news, but addressing HIPPA and today's many other healthcare regulatory requirements may cover only some of an organisation's basic security and privacy needs. It's a good start, but judging by recent news it may not be enough to thwart attacks and keep organizations out of the breach spotlight. More should be done to strengthen security and protect PHI across the whole spectrum of healthcare entities, from hospitals to smaller practices and from insurers to device manufacturers. The way to do more is to make cyber security a business priority.

Protect your enterprise while reducing cost and complexity

From infrastructure, data and application protection to cloud and managed security services, IBM Security Services has the expertise to help safeguard your company's critical assets. We protect some of the most sophisticated networks in the world and employ some of the best minds in the business.

IBM offers services to help you optimise your security program, stop advanced threats, protect data and safeguard cloud and mobile. IBM Security Framework and Risk Assessment can assess your security capabilities across common industry standards by using tools to identify gaps in controls, score your level of IT risk and prioritize remediation activities. IBM Incident Response Planning can help you structure a cybersecurity incident response plan (CSIRP) that incorporates the processes, tools and resources you need to respond to and help reduce the impact of a cyber attack. Should you experience an IT security breach, IBM Emergency Response Services can provide real-time onsite support, including intelligence gathering, containment, eradication, recovery and compliance management. With IBM Managed Security Services, you can take advantage of industry-leading tools, security intelligence and expertise that will help you improve your security posture—often at a fraction of the cost of in-house security resources.

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

Arecont Vision Megapixel Cameras Increase Situational Awareness At Vietnam's Newest Healthcare Facility

Introduction

The City Internaitonal Hospital (CIH) is a new multi-specialty hospital located within the Binh Tan district in Ho Chi Minh City, Vietnam. Located in the international Hi-Tech Healthcare Park, CIH features the latest medical technology and imaging equipment.

With a large volume of visitors anticipated at the hospital every day, the need for a best-in-breed surveillance solution was a high priority from the onset of the project. To fulfil this requirement, hospital administrators turned to Citek Corporation, a technology integrator located in Ho Chi Minh City.

Challenge

The need to secure CIH by maintaining the highest levels of situational awareness was a primary design objective for the new video surveillance system. To achieve this goal Hoa Lam's management team worked together with Citek's technical personnel to design and install a superior video surveillance system.

The decision to deploy an IP surveillance solution featuring Arecont Vision megapixel cameras was based on superior functionality and image quality, ease of use, and the ability to manage the system centrally or remotely.

Megapixel solution

Citek became an Arecont Vision installer in Vietnam in 2009, and installation of the video surveillance system was a smooth process by the experienced integrator. The video surveillance system at CIH is monitored on a local network, which includes a main server and two client systems. There are approximately 200 Arecont Vision cameras installed at the facility to date, including approximately 100 SurroundVideo 360 degrees AV8365DN 8-megapixel (MP) panoramics and 35 SurroundVideo 180 degrees AV8185DN 8 MP panoramic cameras. These high-performing cameras deliver exceptional situational awareness in both day and night lighting conditions. Additionally, there are approximately 60 Arecont Vision MegaVideo AV2115DN compact day/night megapixel dome cameras installed at key locations, which are operational 24/7.

"The quality of Arecont Vision cameras more than satisfies our requirements for image quality," said Mr. Lai Voon Hon, General Director of Hoa Lam-Shangri-La. "The system is working very well for us and Arecont Vision is extremely responsive to our needs."

Conclusion

The CIH management team carefully evaluated their long-term return on investment (ROI) comparing IP and analog surveillance system solutions. Since a smaller number of Arecont Vision megapixel cameras provide superior area coverage to conventional cameras, substantial savings are derived. This includes reducing the number of cameras, cables, poles, and housings plus the requirement for less on-going maintenance and fewer VMS licenses.

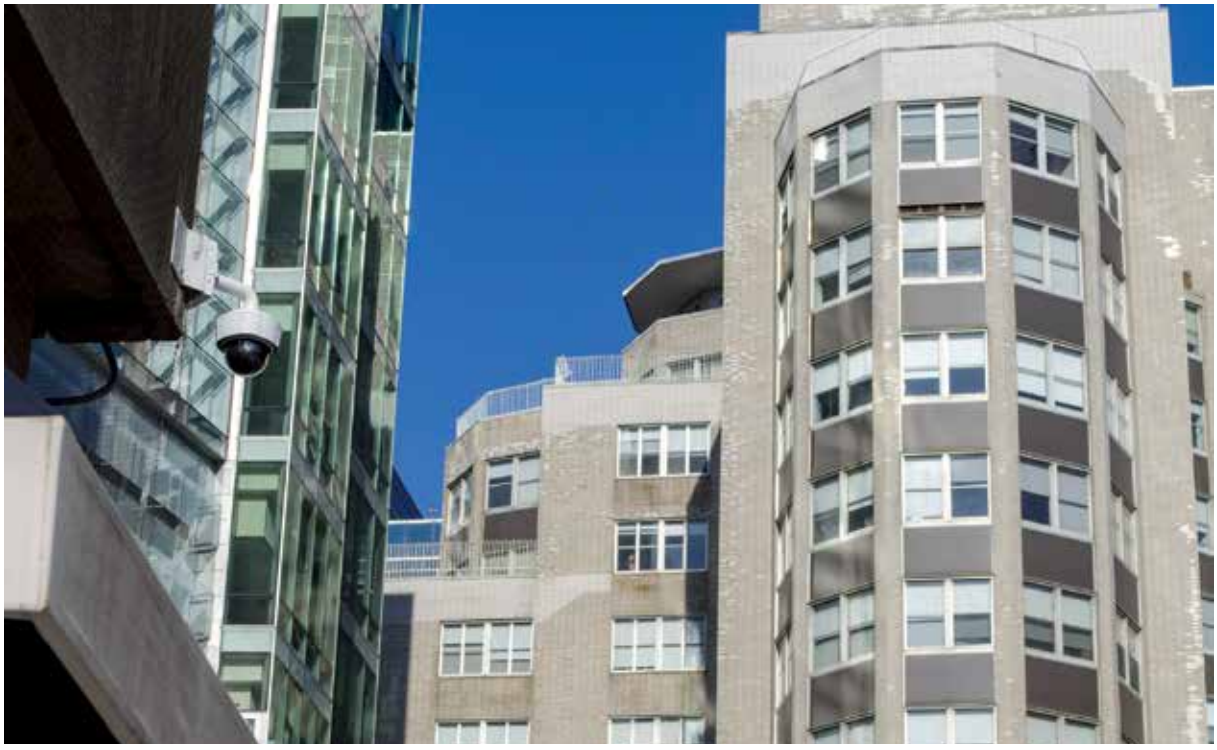
Additional savings are derived from the reduction in manpower needed to watch video feeds and guard

the facility. Beyond the financial benefits, CIH management recognizes the intangible ROI achieved from maintaining high security, which makes the facility a safer place for patients, staff and visitors.

"The International Hi-Tech Healthcare Park will be the first integrated healthcare development in Vietnam to provide a comprehensive healthcare environment employing high tech medical equipment and a professional medical staff. Our new video surveillance system is an important element of that environment," said Mr. Lai Voon Hon.

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

IP Cures Aging Surveillance System With Axis Video Encoders



Introduction

Located in downtown Boston, Massachusetts, Massachusetts General Hospital (MGH) is one of the premier medical facilities in the United States. Its security team is responsible for the safety of over 40,000 people each day. To help support their security efforts, the hospital wanted to upgrade their aging analog security system to an IP-based infrastructure. However, replacing over 600 analog cameras at once was far too cost-prohibitive. MGH needed a solution that could prepare them for the future while maintaining their legacy investments.

Solution

Working with Boston-based system integrator and Axis' partner, Pasek Corporation, MGH decided to replace their DVRs with Axis video encoders. The encoders would network-enable the analog cameras and create an IP-based system on which the hospital could run an advanced Milestone XProtect VMS, as well as analytics by Briefcam. After upgrading with encoders, the hospital expanded their surveillance coverage by installing new Axis network cameras throughout their campuses.

Result

By upgrading to an IP-based system with Axis video encorders, the MGH security team gained increased flexibility in camera management. They are able to customise camera views on the fly and instantly call up video from anywhere on the network. They were also able to eliminate a large amount of equipment and greatly simplify the system's backbone. By further expanding coverage with Axis network

cameras, MGH can now achieve high-resolution video anywhere in its facilities. This is because, an IP-based system allows cameras to be added one at a time, the hospital can continue to add the latest security technology without overhauling its infrastructure.

Securing a city within a city

Ranked as one of the premier hospitals in the United States, Massachusetts General Hospital is a world-renown medical facility that provides cutting-edge care in almost every medical discipline. Its reputation for quality and innovation draws patients, medical professionals, and researchers from all across the globe to the Greater Boston region. Robert Leahy, senior manager, systems and technology for MGH, estimates that upwards of 40,000 to 50,000 people can be onsite on any given day.

"It is a city," he said, and the hospital faces the same range of security challenges – from theft to car accidents to physical altercations. "MGH police and the security department have more licensed officers than my hometown. That's the scope of what we're dealing with. It is anything and everything."

To help keep patients safe in such a busy and sensitive environment, MGH security relies on the support of hundreds of analog surveillance cameras installed throughout its facilities. However, the complex DVR-based system was becoming out-dated and unwieldy to manage. Operators had little flexibility to customise camera views and relied on paper lists in order to call up cameras. Searching through archived video could take hours, and the amount of DVRs, switches, servers and PCs that were required ate up valuable real estate.

Newer IP-based options offered ways to streamline camera management, reduce equipment and give the MGH security team more advanced features with greater control. However, replacing every camera and DVR was far too cost prohibitive. The hospital needed a solution that could bring their surveillance system into the future while protecting their legacy investments. After extensive research, Leahy decided to migrate to IP by replacing his DVRs with Axis video encoders. The encoders would provide an immediate upgrade by network-enabling his existing analog cameras and create a platform for future growth.

"We had over 600 cameras," Leahy said. "It would have been too costly to replace every one of those, but going the encoder route was such an easy deal."

Encoders bring simplicity

Leahy enlisted Boston-based systems integrator and Axis partner Pasek Corporation to undertake the digital conversion. The project encompassed the entire MGH system, including the 999-bed main campus in downtown Boston, the research center at the Charlestown Navy Yard and satellite locations in the nearby cities of Chelsea, Revere and Danvers.

Pasek began by swapping out the DVRs for 16-channel AXIS P7210 Video Encoders. This greatly simplified the system's backbone. Before the upgrade, the 400+ cameras at the Boston campus ran through 25 six-inch tall DVRs mounted on four 84-inch tall racks. Switching routers directed the video from the DVRs to monitors for live viewing only on designated computers. The video was then sent to a separate server system for storage due to the risk of DVR hard drive failure.

After upgrading to IP, the two-inch Axis video encoders manage the same number of cameras at a third of the rack space. Furthermore, the encoders send the signal straight to a server running a Milestone XProtect VMS. There, it can be accessed through the network by any approved device with the Milestone client.

"The amount of devices and power supplies they were connecting shrunk by 75 per cent," said David Alessandrini, vice president of Pasek Corporation.

Saving time while saving lives

By running their system on the Milestone platform, the security team broke free of the previous limits on camera views. Whereas before, monitors were locked into pre-set camera groupings, the Milestone VMS can create custom groups on the fly. The IP upgrade also eliminated time-consuming procedures to call up cameras and search archived footage. Now, operators can pull feeds from anywhere on the network with a click of a mouse, and investigators can download video by simply entering the time and location desired.

The open nature of the IP solution lets the hospital install analytics such as the Briefcam video synopsis software to compress hours of video into just a few minutes. This will help the hospital conduct sophisticated analyses to improve both security and business operations. Leahy mentioned their parking managers are already excited for the information Briefcam will provide.

"There are so many different things we can do with the IP system," Leahy said. "It makes life so much easier."

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

Axis Network Cameras For Intelligent Maternity Care

Introduction

The Primorsky Regional Perinatal Centre is a leading healthcare facility located in Vladivostok, providing care services for women during pregnancy and childbirth. The Centre is fitted out with cutting-edge treatment and diagnostic equipment and widely known for its professional approach even to high-risk patients. Security in such a facility is certainly one of the highest priorities that can be supported now by intelligent network cameras with analytic capabilities.

The implementation of the video surveillance solution in the PRPC was also challenged by severe climatic conditions in this region: outdoor cameras should withstand strong winds and snowfalls in the wintertime, high humidity in the summertime and the temperature range of -35 degree Celsius to +30 degree Celsius.

Solution

The customer decided to install Axis IP cameras and the midspans (power supply units for cameras with PoE) due to their numerous advantages, including sophisticated technologies and high reliability, high resolution, low maintenance costs, scalability and integration into a common Structured Cabling System (SCS) and LAN. Moreover, this Axis solution was selected due to its enhanced analytical capabilities, including motion detection, cross line detection, etc.

Result

Today, the entire area of the Centre and adjacent areas are securely monitored by the video system, both indoors (entrances, corridors and critical areas) and outdoors (perimeter and gatehouse). Also, Axis PTZ cameras are installed in all critical elevations. Video streams from all monitored areas are broadcast to security rooms, archived and may be promptly retrieved when necessary.

Implementation features

Originally, the main reason for implementing a network surveillance system in the Centre was to comply with inside and outside security and safety requirements. This high-performance system must operate continuously and trouble-free in severe climate conditions, which means both failure-free operation and sustained high video resolution.

Eventually, new advantages of the network devices with analytics capabilities became apparent. First, these are built-in camera functions, including Gatekeeper (the camera moves and tracks a moving object), Cross Line Detection, auto alarm in case of vandalism, etc. Also, the Axis open platform provides the ability to install numerous video applications. These functions are

intended to apply in the future.

System control

The SecurOS software package developed by ISS was selected as the system core since it is fully compatible with the Axis software and provides a flexible system expansion. This solution provides archiving, monitoring and centralised control of PTZ cameras from a single workstation.

All outdoor cameras are supplied via AXIS T8123 High PoE Midspan 1-port because of high power supply requirements and long cables. This is an innovative technology (Power over Ethernet) that requires no power cables and that supplies power to Ethernet devices using twisted pairs. Thus, time and money is saved on camera installation operations.

The Axis network cameras feature autofocus and back- light compensation functions, as well as automatic date and time settings over the DHCP protocol.

Conclusion

According to the PKPC's representative, Ekker Ltd., a partner of Axis, paid attention to all the details during the design and installation of this new surveillance system. This is the reason why no incidents have occurred since the installation of the network cameras. Operators monitor the situation from the central security station while senior managers can retrieve any archived video records and view them in HD. After the available intelligent system functions are used more intensely, the Center's personnel will be able to focus on critical areas and entrust the Axis cameras with everything else.

The Primorsky Regional Perinatal Center in Vladivostok has gained an excellent reputation among its patients; the Center intends to go further and install additional Axis cameras.

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

Or Yom Nursing Home Secures With Tyco Security

Introduction

Developed under the auspices of the Neve Shalom Jewish Synagogue Foundation, the Or Yom nursing home was opened in September 2004 under the name Barinyurt.

Challenges

The nursing home spans two buildings over 11 floors – a newer facility in which a nurse call system could be more easily installed and an older building that presented more challenges when designing and installing a system because of its thick walls and room configuration.

For both buildings, it was important to devise a system that would let the caregivers and nursing staff know the location of each resident and provide those residents with a means to send an alert in case of an emergency. The nursing home also wanted to put more technology in the hands of staff, giving them the ability to send alerts if they were in distress.

Solution

Working with its integrator Sigmamed, the nursing home deployed the Elpas Real Time Location System (RTLS) for its 130 residents. Each resident was issued a healthcare positioning tag that serves as an active RFID transmitter.

The tags work in conjunction with a series of readers installed throughout the facility. For this project, Sigmamed took different approaches based on whether it was woking in the older or the newer building.

Within the older building, which had walls that were more than 2 feet, 7 inches thick, the integrator installed infrared (IR) readers in each of the residents' room. This part of the facility offers a shared bathroom on each floor, so a single low-frequency (LF) reader was positioned at the entrance to each bathroom.

The older building also houses a main dining hall, so a single radio frequency (RF) reader was positioned in the centre of the hall so it could cover all the elderly residents gathered there.

The new building, with more modern construction, allowed Sigmamed to put LF readers in individual resident rooms, near each entrance. This way, if a resident issued a call for assistance, the staff could easily see the room from which the call is coming and respond, whether the person was in the en suite bathroom or in the general living space.

Within the facility's Alzheimer's unit, readers were positioned so if a resident attempts to wander beyond the confines of the floor, an alarm is sounded.

Resident tags are monitored via computers situated at three nurses' stations. Here, nurses can monitor distress calls from the elderly, with the system providing positioning information. The nursing staff also has the option to receive calls on a mobile phone in case they are away from the nurses' station.

The 20 doctors, nurses and caregivers at the facility were outfitted with active ID badges so their movements can be monitored as well. The staff tags also serve to cancel an alarm once a staff member responds to a request from a resident through an automatic action within the badge. The information transmitted from the staff tags aids in tracking response times and gives the head nurse information on who has responded to an event.

If a caregiver needs additional help, the badge serves as a means of sending a Code Blue just by a press of a button on the badge.

Another feature available to staff is the ability to monitor calls and information through an easy-to-use mobile application from Elpas called Eiris Go. The app can track such activities as nurse calls, duress alerts and wandering residents.

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

Health Care System Boosts Security And Unifies Video Management

Introduction

St. Joseph's Healthcare London has a history dating back to 1869. The Catholic healthcare organisation is governed by St. Joseph's Healthcare Society of the Roman Catholic Diocese of London, and its services are publicly funded. Today, the hospital system, which consists of four major sites and more than 3 million square feet of space – is one of Ontario, Canada's leading teaching hospitals. Renowned for compassionate care, St. Joseph's is one of the best academic healthcare organisations in Canada dedicated to helping people live to their fullest by minimising the effects of injury, disease and disability.

Together, St. Joseph's Hospital, Parkwood Institute, Southwest Centre for Forensic Mental Health Care, and Mount Hope Centre for Long Term Care comprise the hospital system, which has an annual operating budget of more than $400 million.

Affiliated with the University of Western Ontario (Western University), St. Joseph's annually hosts approximately 2,000 residents, clinical fellows and other health discipline students from colleges and universities around the world. Its 4,044 employees and 900-plus physicians complete approximately 22,148 day surgeries and 34,321 urgent care visits yearly.

St. Joseph's Security Control Centre handles all emergency calls for the entire organization 24/7 and responds to potential acts of violence, fires, bomb threats, medical emergencies, missing patients, inclement weather, chemical spills, evacuations and critical infrastructure failures. In addition, security personnel monitor the organisation's expansive surveillance system to help ensure the overall safety of patients and employees.

Challenges

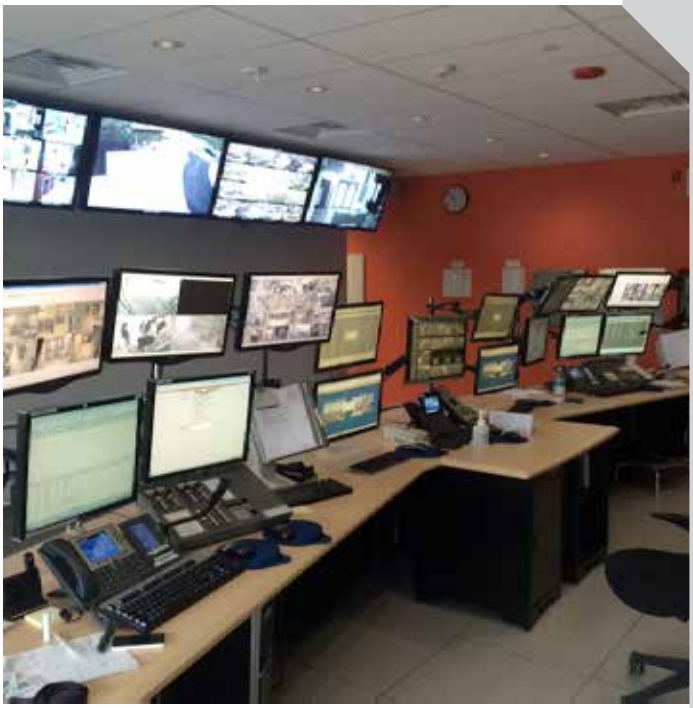
St. Joseph's security program began with a small VHS recording system more than two decades ago. Over the years, a stronger emphasis has been placed on ensuring the safety of St. Joseph's equipment, employees and its patients, and as security technology has evolved, the hospital system's surveillance system has advanced and expanded as well.

The organisation recently decided its analog video surveillance system was in need of an upgrade to IP technology. Because St. Joseph's Hospital was planning a renovation and wing addition, the security staff chose this facility for a new system.

St. Joseph's security team had been experiencing delays in playing back videos, said Mike Bessegato, director of Fire & Security Services/Emergency Planning at St. Joseph's. "We were not able to find and review the right video footage quickly enough in the event of an incident," he said. "And with analog cameras, you're definitely limited in terms of being able to see people clearly and identify them." On the hospital's wish list for an upgraded system was real-time viewing, more detailed images and the ability for operators to simultaneously view more than six cameras per screen in the control centre.

One of the challenges that Bessegato and his team wanted to address was St. Joseph's unique security and surveillance requirements for different areas and facilities within the organisation. For example, the hospital system's mental health facilities require nearly 100 per cent surveillance coverage to provide protection for both the staff and patients.

Other monitored areas range from public corridors where pharmaceuticals are housed for emergencies to remote parking areas. But the needs did not end there. The Security Control Centre takes in approximately 500 calls in an eight-hour period, so security officials required a system that would enable staff to respond to a high volume of calls while providing a safe and secure environment for patients, staff and visitors.



Solution

With its security needs laid out, the organisation's integrator of more than 20 years, Integrated Video & Surveillance Inc., presented St. Joseph's with a plan to bring the hospital system into the IP world and position it for the future.

"I've been here 22 years now, and Integrated Video & Surveillance Inc. has been maintaining our cameras ever since," Bessegato explained. "They continue to bring forward the newest and latest technology and have helped our security system evolve--particularly as St. Joseph's has grown and security has become bigger and more important within the organisation."

Because Bessegato and his team of 60 were looking for a similar user interface to their current video management system, along with strong analytics and better resolution, the integrator ultimately recommended the VideoEdge video management system from Tyco Security Products' American Dynamics brand. Together, with more than 45 new Illustra IP cameras, the security platform would allow St. Joseph's to realize the capabilities of IP, while seamlessly managing current analog cameras that they were not quite ready to upgrade. Overall response time would be faster, and operators in the control center would be able to view 32 cameras on one screen.

Previously, operators had only been able to view six cameras at once.

While St. Joseph's previous video management platform allowed security personnel to view real-time video, they had been experiencing latency, along with interruptions during playback. "The VideoEdge VMS allows us immediate playback and real-time viewing, allowing our guards to react to events as they happen," Bessegato explained. In addition, he said, no latency means security personnel can follow people from camera to camera more smoothly, and the high-definition resolution allows for much better image quality.

"Another pro we found is that we can capture still images from the video review without having to save the video clip first. That has been an important bonus for us to be able to immediately export a face or license plate without taking additional steps," Bessegato said.

The organization's 600+ cameras are used to manage slip and fall incidents, equipment theft, and even to make sure areas have been salted during the winter to prevent potential accidents. "High-resolution cameras can spot these things, and dispatchers can work very efficiently this way," said Tim Hobbs, managing partner at Integrated Video & Surveillance Inc. For example, one recorded incident in a facility parking lot showed a driver backing into another car and leaving the scene. The resolution was high enough to provide staff with clear images of the incident and driver's license plate, Hobbs explained.

Security personnel have also benefitted from other capabilities such as sophisticated analytics, made possible by the powerful victor client used with VideoEdge. "With the victor client, St. Joseph's can count people going in and out of a building to estimate traffic on the floor, and they can analyse which corridors or entries are being used more. They can also set restricted areas that will cause an alarm to pop up for security personnel if someone is walking into a controlled area," said Hobbs.

Although St. Joseph's has one control centre, staff can also view video at individual locations via PC and remotely. The VMS allows security personnel to send live video to other monitors or personnel at other sites, allowing guards across different cities to react to an event very quickly.

Hobbs added that the VideoEdge VMS with victor has allowed St. Joseph's the flexibility to prioritise not only which existing equipment needs to be upgraded, but also the flexibility to choose the type of cameras they need for a particular solution. "For instance, in some areas of the new hospital wing, we wanted high definition for facial recognition in an entryway. In other areas where we just needed eyes down a long hallway, for example, we could use a lower-budget option and save some money," he said. "It's nice to have a system that allows you to prioritise your surveillance needs, while integrating it all together seamlessly – it allows us to design a very complete video system that way."

Conclusion

Though St. Joseph's new security platform will allow it to upgrade the entire surveillance system over time, the ultimate intention is to get there sooner rather than later.

"Our goal is to be completely digital as soon as we can," Bessegato said. "The benefits we see so far with the video management platform and IP cameras have been paramount. IP augments so many of our other procedures and has been very beneficial to our organisation."

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

secutech
VIETNAM

Vietnam's Largest and Most Professional Exhibition
and Conference for Security, Fire & Safety

Vietnam No. 1
Your Profitable Choice and Flagship Show

21 — 24 September 2016
Friendship Cultural Palace, Hanoi, Vietnam

www.secutechvietnam.com

Global contact
Messe Frankfurt New Era Business Media Ltd (Taiwan Branch)
Ms Echo Lin, Manager
Tel: +886-2-8729-1010
Fax: +886-2-2747-6617
Email: stvn@newera.messefrankfurt.com

secutech Vietnam

VIETFAIR

messe frankfurt

Dana-Farber Cancer Institute Manages Ever-Changing Security Monitoring Needs With Tyco Security Products

Introduction

The urban campus of Dana-Farber Cancer Institute in Boston is representative of many modern metropolitan healthcare institutions today, with a main campus in a busy city centre that takes advantage of every available square inch. New buildings replace existing structures, existing facilities are reconfigured, and as the institutions continue to grow, their footprint expands into surrounding suburbs in an effort to serve their growing patient and research needs.

Internationally renowned for its unique blending of clinical and research operations to provide state of the art cancer care — the institute supports more than 300,000 patient visits annually and is involved in some 700 clinical trials — the only constant for Dana-Farber is change. In addition to the four satellite locations in greater Boston

and the main campus in the city's Longwood medical area, the institute also maintains clinical affiliations and a physical presence at other high profile institutions, such as Brigham and Women's Hospital, Children's Hospital Boston and, Harvard University, further expanding the institute's reach.

When Dana-Farber undertook its most significant expansion project to date, the design and construction of the institute's new Yawkey Centre for Patient Care, the project included demolition of two existing buildings and a street-level parking lot at its Boston headquarters to make room for the new 14-story building. Dramatically expanding the institute's clinical care space, the new Yawkey Centre features more than 100 exam rooms, 150 infusion spaces, and 20 consultation rooms. Built around a philosophy of uniting clinical care space with related research functions, the institute fosters collaboration and information sharing about particular cancers and treatments.

Challenges

During the three-year construction, security and facilities management staff had to evaluate the impact of the new state of the art facility on the current and multi-location infrastructure. Not only did the Yawkey Centre add an additional 275,000 square feet of clinical and support space to the institute's overall footprint, but security plans for the centre included the addition of nearly 200 additional IP cameras that had to be seamlessly and efficiently married with Dana-Farber's significant investment in their current CCTV surveillance equipment.

With 23 existing Intellex DVRs from American Dynamics and nearly 300 analog cameras already deployed throughout its facilities, Dana-Farber security staff were searching for a solution that would allow dispatchers in its security command centre to have a single interface through which they could view live and recorded feeds from both analog and IP cameras.

"Running two separate systems for analog and IP video was just not an option for us to deploy into our security monitoring operations," said Ralph Nerette, Manager, Security for Dana-Farber Cancer Institute. "The solution we chose had to be seamless for our dispatchers to be trained on and successfully use, regardless of whether video is coming from the DVR or NVR environment."

Complicating this search were some additional responsibilities that Nerette's security staff was about to assume. As part of an overall renovation and upgrade project, central dispatch functions for facilities maintenance, housekeeping and environmental health and safety were about to become part of security operations. Coined the institute's Facilities Security Operation Centre (FSOC), this facility would manage Dana-Farber's two million square feet of clinical, research and administrative space and a call volume that sometimes exceeded 1,000 calls per day, requiring significantly more infrastructure than the current 120-square-foot security command centre could handle.

"We needed much more functional space and the ability to segment equipment, reduce noise and allow our dispatchers to focus on customers and provide the level of service required of a security operation of this size," Nerette said.

Solution

With such a large, functioning network of Intellex DVRs, Nerette and his staff worked with systems integrators Tesla Systems, of Georgetown, Mass., and Team AVS of Westford, Mass., to find a VMS solution that would allow the DVRs to be used in tandem with the new IP-based cameras and NVRs, as well as function as a platform for the future as the institute eventually migrates to a fully-IP-based solution.

Using the new victor unified video client and VideoEdge NVR from American Dynamics, all IP and Intellex DVRs' analog video streams from Dana-Farber's 500 cameras are seamlessly integrated into victor's single system and user interface. Instead of toggling between different applications on their monitors, dispatchers can be concerned only about the content of the video and fulfilling their regular duties of ensuring the safety and security of the hospital facilities and not what recording technology the video is being generated from.

"This approach allowed the institute to extend the life of our existing Intellexes," Nerette said. "Rather than rip and replace, we were able to focus our new investments on state of the art IP technology as part of the Yawkey expansion. This let us strategically add IP cameras in additional key areas and save money," Nerette said.

The 200 new IP cameras from The Yawkey Centre and a handful of other camera clusters, such as a small, 22 IP camera deployment in one of the more sensitive research areas, are recorded on four VideoEdge NVRs from American Dynamics, with two NVRs for fail-over to ensure no interruptions in operation. On average, Dana-Farber will be storing 30 days of video per camera on the institute's 70TB of external iSCSI storage.

With dispatchers viewing some 60 cameras view up at any given time, those unified operations are crucial to the workflow of the command centre, according to Robert O'Rourke, Account Executive, Tesla Systems.

"One of the unique challenges of this project was to integrate the analog and IP video technologies to make them function seamlessly together," O'Rourke said. "The command center has two 42-inch monitors and 14 other 20-inch screens, with video coming in from five remote locations, so there was a lot of complexity."

Another essential requirement of the system was the ability to easily share video with other users within Dana-Farber, all while safeguarding unauthorized views and exports of the footage. With victor's embedded policy management functions, Nerette is able to grant secure access to other users of the CCTV system – outside of the security and facilities maintenance divisions – to view video from specific live feeds or recorded video only from other areas of the facility from designated cameras. These groups also cannot export any video as part of the victor policy management deployment.

Security staff in the institute's command centre will soon have even one less standalone system to monitor. With an upgrade to Software House's C•CURE 9000 security monitoring platform planned for sometime next year, Dana-Farber will be able to use victor's upcoming 2012 release as a single unified event and security management platform to integrate the card access functions, as well as fire and other building management functions, according to Geva Barash, president, Team AVS.

Conclusion

It is clear to Dana-Farber staff that undertaking the deployment of a new command center, built around the victor platform that harnesses the strength of Dana-Farber's existing video infrastructure and the flexibility of IP video, has accomplished two major goals. Not only has it provided the institute with a custom designed clinical facility to further its mission of excellence in cancer care and research, but also a state of the art infrastructure on which to base security and facilities operations for the future.

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

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

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

Opening the Doors towards Innovations in Building Maintenance, Facilities Management and Green Building

Expected trade visitors
10,000

International presence
36 countries

Exhibit area
6,750 sqm.

Expected delegates
1,500

Contact us now to BOOK YOUR SPACE!

Mr. Chanon Ekarattanakul (Thailand)
Tel: +66 (0) 2833 5208
Email: chanone@impact.co.th

Organizers

IMPACT MUANG THONG THANI

sphere exhibit
A SUBSIDIARY OF

A part of Asian Construction Week

ASIAN CONSTRUCTION WEEK

Singapore In Keeping Up With Global Security Trends

Information contributors:

Anmol Singh, Principal Research Analyst, Gartner

Derek Chew, General Manager, Soverus Consultancy & Services Pte Ltd

David Siah, Country Manager, Trend Micro Singapore

Introduction – How much has security changed in Singapore over the last decade?

Singapore and all of its modernity has positioned the nation as one of the most technologically advanced nations amongst its ASEAN peers. As we put Singapore's security landscape in focus, it has most definitely grown "significantly" over the last decade, according to Principal Research Analyst at Gartner, Anmol Singh. With global security issues like terrorism and militant groups like the ISIS causing terror attacks at almost every corner of the world, Derek Chew, General Manager of Soverus Consultancy & Services Pte Ltd agrees that security efforts are definitely a priority to governmental organisations in Singapore.

Chew says that, "The terror attacks of September 11 had an immediate and substantial impact on Singapore." Sharing his observations, after the 9/11 attacks, Chew explained that, "Authorities enhanced security trainings for all security personnel in Singapore. Other related security services like security systems and security consultancy services saw a huge increased in demands."

Moving forth to the cyber security arena, there have been increasing concerns in many major organisations from various industries in Singapore on protecting valuable data. David Siah, Country Manger of Trend Micro Singapore gives us an insight what to expect from the cyber security realm in Singapore. "The past decade has seen tremendous change in Singapore's cyber security landscape, its IT adoption, and cyber awareness."

Referencing from the Infocomm Development Authority of Singapore (IDA), Siah feels that, "Singaporeans are becoming more security-conscious and tech savvy, with eight out of ten taking measures to ensure that their personal computers were secured by installing anti-virus software and security updates." However, when it comes to mobile devices, Siah concludes that the number of people concern over their information safety is relatively lower.

Siah also analyses that, "Over the years, the local cyber landscape has been increasingly flushed with various types of cyber attacks of which, the most notable one is the attack that took down Ang Mo Kio Town Council and PAP Community Foundation's websites, initiated by an anonymous hacktivist group."

Singh however feels that Singapore has yet to properly keep up with the business and technology innovations the industry has witnessed. Agreeing with Siah from Trend Micro Singapore, Singh deciphered that, "With one of

the highest penetration rates globally of smart devices in everyday lives of Singaporeans, the government agencies and businesses have been constantly challenged with the rising level of threats to safeguard citizens and customer information." Important and prized information are constantly at a risk of being hacked by outsiders or insiders themselves but to Singh, "A number of measures undertaken to contain the risks emanating from an increased uptake of mobile, cloud and IoT technologies have not been able to offer the expected value due to the hindrances ranging from lack of sustained budget to effective execution."

Trends development in the Singapore security landscape in 2016

Singh predicts, "Singapore is going to see an increased awareness about security and privacy among its citizens and how they interact with businesses and government on a regular basis." Additionally, Singh also foresees, "an accelerated growth in IoT deployments to support the smart nation initiatives, government agencies and other organisations are going to adopt a converged security approach that address the issues with data exchange and IoT devices."

In the area of physical security, Chew points out that, "Although video surveillance technology has been around for approximately half a century, it has only recently become a viable replacement for the more conventional forms of security. For example, for sensitive areas that require controlled access, it has always been taken for granted that physical security officers are preferable to CCTVs or other forms of video surveillance. However, with the introduction of cloud-based technologies and higher bandwidth communication, modern surveillance has overcome the onsite, low-quality video limitations that were once unavoidable."

Chew anticipates that the security trends in Singapore will move toward, "replacing manpower security with security technology." Justifying his prediction, Chew says, "Video monitoring is less expensive as compared to hire security officer to protect one's premise because it requires a complete rotating team of officers and each officer requires equipment, training and insurance." Continuing the analysis to his foresight, Chew adds that, "Video monitoring never sleeps on the job, even the most vigilant guards have a tendency to lose focus when faced with long and uneventful hours. Top-of-the-line remote video monitoring uses intelligent recognition software to identify threats as soon as they appear, alerting the monitoring team and initiating deterrent procedures within moments of initial contact. Video monitoring never loses focus, which means that your premises will be as well protected at 3:30am, as it is at 1:30pm."

Within the cyber security field, Siah anticipates three major security trends emerging and all of which will potentially impact the populace in different ways. "The first one," Siah expressed, "would be online extortion, whose modus operandi is evolving to manipulate a victim psychologically. For example, cyber criminals might use fear to coerce a victim into paying for non-disclosure of his/her personal information."

Siah then goes to the second predicted trend that are "increasing attacks targeting organisations that are moving to or using cloud services. According to F5 and Frost & Sullivan, 91 per cent of organisations are already utilising cloud services or have the intention to use them. In Singapore, almost 40 per cent of enterprises

are using cloud computing while more than 35 per cent are planning or implementing cloud strategies. The catch here is, cloud security is very different from legacy software protection, and thus it takes an entirely different security approach."

The last trend that Siah sees growing in the cyber security area is, "mobile malware, becoming a rampant issue – the total number of malware is projected to hit 20 million by end of 2016. In Singapore we have seen several cases of hacked phones manipulating transactions via banking apps, leading to loss of thousands of dollars for the victims. As mobile payment steadily rises, hackers will increasingly develop mobile malware targeted at mobile payment applications. In such scenarios, cybercriminals are able to use social engineering techniques to lure victims into surrendering important information or clicking on malicious links and subsequently installing a malware on their phones. The hacker could then take control of the device, and conduct illicit acts."

Singh echoes both Siah and Chew's analysis for Singapore's future trends. "As we see an accelerated growth in IoT deployments to support the smart nation initiatives," Singh says, "government agencies and other organisations are going to adopt a converged security approach that address the issues with data exchange and IoT devices. As smart-city departments deploy IoT systems, increased data flows will require city department CIOs to update their data and information, strategy, management culture and processes. With the proliferation of these devices to support digital business and even traditional business models comes a profound increase in the "surface of threat" in technology infrastructure and services."

Furthermore, Singh deduced that, "As critical infrastructure industries such as telecommunication and utilities operating in Singapore embark on IoT initiatives in 2016 and the years to come, in order to transform their business models and deliver new products and services, a pattern of security challenges and potential failures begin to emerge. Security leaders will be required to address these emerging security challenges with approaches that address OT (Operational Technology) security issues, including dealing with regulatory compliance and performing risk assessments across the OT and IT systems."

Singapore and embracing latest security trends in the market

Being a technologically advanced nation, Singapore tries to keep up with almost anything innovative and superior but this does not necessarily mean that it is a good thing. Singh says, "Given its already technologically advanced ecosystem relative to other SEA nations, Singapore is an early adopter of technology in the region that not only widens the attack surface and makes it vulnerable to new types of threats, but also opens up new business opportunities."

Chew feels that, "Businesses in Singapore are increasingly seeing the benefits of analytics to provide proactive surveillance to protect their businesses as well as cost saving by using technology to reduce manpower cost." According to Siah, "Singapore has one of the highest percentage of Internet users, compared to its global counterparts. As seen in the same IDA survey, Singaporeans are increasingly aware of cyber-security pitfalls, and have taken some measures to protect themselves. However, there is still room for improvement."

Singh's analysis cover grounds on how there is a growing interest in small and mid-sized organisations operating in Singapore to consume cloud and mobility services for business critical operations to provide cost effective and consumer friendly solutions. "We also see increased adoption of intelligent and context-aware security events by gathering and analysing a broader set of data, such that the events of relevance that pose the greatest harm to an organisation are found and prioritised with greater accuracy," Singh continued explaining.

Security trends in Singapore impacting the global market and vice versa

Gartner's research analyst, Singh identifies that, Singapore has always been "consistent with the regional and global security trends. Organisations in Singapore are increasingly acquiring new cyber security skills, vendor products and services to embrace an adaptive security architecture for protection of their information assets and consumer interests from the emerging threats."

Supporting Singh's opinion, Chew analyses that, "Singapore presents itself as a choice location as an international hub." Chew continues, "Many cities around the world such as Mexico City, Madrid and Stockholm that have already embarked on similar Safe City Initiatives. They have deployed integrated and interoperable security systems across several agencies to optimise the response from detection to action."

Singapore can learn from these countries that have begun to start their initiatives into making their cities a smart one. It will thus help to develop the safety and security industry in Singapore. Chew justifies, "This will help government agencies or businesses to develop new analytical capabilities with an improved and combined operating picture, enhancing situational awareness and decision making."

Even in the cyber security sector, Siah says, "Singapore, within the Asia Pacific region, is considered a bellwether in terms of adopting new cyber security technologies and educating the masses about its importance. Having established itself an exemplar, less cyber security-mature countries in the region will follow suit. For example, the Singapore government previously organised an ASEAN workshop to discuss bilateral cyber security negotiation processes and how the region can move forward in terms of cyber security policy."

Basically, Singapore is dependent on how the global security market works. Siah feels that, "Living in a connected modern world means information travels fast, and lessons are learnt on a global level. Several high-profile cyber attacks such as Sony Pictures Entertainment and JP Morgan breaches, have taught Singapore to start shoring up cyber security defences before anything bad happens.

Conclusion

Singapore is pretty much known as the nation that does not compromise on their security entities. The country embraces security in its most advance form to ensure our borders, hospitals, airports, buildings, residential spaces and other areas are fully secured and safe for visitors, residents and workers. Singapore does not take safety and security for granted, equipping the island with the prepared mentality to take drastic measures should any sort of breach of security occurs. SST

Hotel Security Enhanced With Key Control Systems

Attribute to:
Fernando Pires,
VP Sales and Marketing,
Morse Watchmans

The National Crime Prevention Council emphasises that preventive security measures are crucial to keeping hotel guests safe against crime. According to their website, "Security is an essential investment and not an optional expenditure." In making the investment in preventive measures, hotels must balance security with the need to create a welcoming environment for patrons and guests.

One of the ways in which hotels are managing this challenge is to strengthen the roles of key control and access control, particularly for sensitive operational areas and for master access keys. Following are a few ways key control can help hotel management achieve a healthy balance between security and guest convenience.

Resource management

Hotels tend to employ a large and varied workforce and many of the staff have job-related reasons to use various facility keys. Kitchen staff cooks with the contents of food pantries and freezers; front desk employees must sometimes open cash boxes or safes; maintenance crews do work in utility rooms and storage closets; etc. It's vital to business operations to allow access to these areas, but not unrestricted access, which could create the opportunity for theft.

Automated key control and management systems offer an easy solution to improving resource management by

automating the process. Facility keys are securely stored in a tamper-proof cabinet and authorised users can only remove a key to which he or she is permitted to use by entering a pre-programmed PIN code. If the criteria entered matches the information stored in the system database, the key cabinet will unlock and the necessary key can be removed or returned.

Tracking

Knowing who has which keys, when a key was taken or when it was returned is fundamental to operational security in the hotel. Key control systems are designed to record all transactions and make the information available in easy to read reports so that management has an automated audit trail of who accessed which key and when. Many hotels require daily audits for keys that are in regular use to meet accounting and loss prevention standards, and information provided by the key control system provides this while saving a tremendous amount of resources in time and manpower.

The reports can be used to trace missing keys, keep better control of assets and help ensure timely follow-up action if there is an incident. If an incident does occur, management can query the system for specific details such as a listing of all transactions between certain times; and when doing a follow up investigation, management can request a report for the hour preceding the incident. Immediately following an incident, a report can be generated showing which keys are back in the system and which keys are still out and who last accessed them. Real-time audit reports can also track keys in use, overdue or lost keys, the location of a stored key (i.e. which key cabinet in the system) and any inconsistent key usage.

System integration

One of the effective ways to optimise key management and access control within a hotel environment is through system integration. A key control and management solution can usually be integrated with the existing physical security system such as video surveillance and existing identification card systems without costly upgrades or overhauls. Advanced communication capabilities enable key control systems to be monitored and administered remotely from PDAs or smartphones as well as from the desktop.

The compatibility with other security systems and network access offers an added richness, while usability and integration with existing databases saves time and money. As an example, when using a common front-end database and programming, transactions such as adding or deleting users are synchronised for easier and more efficient administrative control.

Security

By their nature, hotels are vulnerable to both internal and external risks. From food and beverage fraud to missing keys, from room theft to hotel events with non-guest participants, hotel management must continually be on guard to ensure the safety of personnel and security of hotel assets. The implementation of a key control system can help strengthen security by preventing unauthorized access to a storage unit full of expensive liquor. With comprehensive tracking capability, key control systems can help reduce the incidence of lost or misplaced keys used by staff, participants or vendors during a conference held at the hotel.

Key control systems are designed to improve hotel security in other ways as well. For instance, keys can be returned to any cabinet in the system, but if a key is not returned when scheduled, e-mail alerts and text messages can be sent to selected individuals to enable quick action.

Throughout the hotel, key control systems can help improve operational efficiency and more importantly, the overall safety and security of guests, staff and property.

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

Central Embassy Secured By Bosch Integrated Security Solutions

Introduction

Anchoring Bangkok's most prominent crossroads, Central Embassy is ideally placed as the sole retail development on the busy Wireless and Ploenchit Road junction. This prominence ensures constant passing traffic from the nearby affluent areas. In order to maximise its security systems and secure all their international premium customers, Central Embassy Limited decided to seek the top of the line security solution to meet its top-tier image.

Choosing Bosch

An evaluation was done with a range of key competitor brand systems. Bosch was chosen for its clear images and superb sound quality, which were essential qualities to enhance the entire security performance. The fact that the multi-language option from Bosch's video systems software is also user-friendly with the Thai language advantage.

To ensure the compound was safely secured, a video surveillance solution was proposed with Bosch's fixed and auto dome cameras. Complete with 720p and 1080p HD resolution and live recording capabilities, Bosch cameras are packaged all in an ultra-compact aesthetically pleasing and rugged design that is built to last. All of Bosch's products were installed on 7 floors of Bangkok's premium shopping mall.

In the event of an emergency or any safety threats, a public address system is needed to ensure safety evacuation announcements are loud and clear. The mall decided to invest in Praesideo. The system offers superior speech intelligibility and it is fully programmable and easily integrated with security and safety systems.

The whole installation comprises of 1 Praesideo system, 10 LBB series Power Amplifier (PA2400T and PA2500T) and 424 numbers of Electro-Voice EV ID C8.2 30W 2-way ceiling speaker that is designed for high ceiling to offer maximum fidelity and intelligibility.

Conclusion

Proposed and installed by Patarungroj Ltd., this total solution comes backed by Bosch quality and professional maintenance services. The project team from Central Embassy Hotel Limited – owners of the property have expressed their satisfaction with Bosch products and will continue to use Bosch for the phase 2 of this project.

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

Kinokuniya Equip Stores With FingerTec's Security Measures

Introduction

Imagine the potential threat that could occur to any company should there be an absence in security. No matter the type of organisation or company, security is as essential as the staff, facilities, product, and the branding concept. Ensuring the safety of staff members, facilities, resources, and items from harm lets business runs smoothly with no hindrance to cost and productivity. TimeTec Computing Sdn Bhd deals with access control and time attendance as well as video surveillance, with systems that use biometrics or cloud technology. These systems are designed to be user friendly and cater to any company no matter the size and industry.

The retail industry is prone to suffer damages and loss due to the environment that such businesses are placed in. This case study will look at three businesses that use access control and time attendance to provide security to their premises while also implementing a workforce management system.

The challenges, solutions and results

Kinokuniya is a renowned international bookshop chain from Japan, founded in 1927, with its first store located in Shinjuku, Tokyo. Recognised as AsianBasis Sdn Bhd in Malaysia, the company serves as the online retail division of the Books Kinokuniya group. With more than 80 stores in Japan and overseas, Kinokuniya stays ahead of its competitors by stocking up on over 20, 000 book titles from both the Japanese and international publications as well as art books, magazines, DVDs, CDs and stationery.

The Malaysian Kinokuniya outlet is located at Suria KLCC, a prestigious shopping mall located in a high volume commercial area, which sees an average of 100, 000 visitors daily. As such, keeping track of the attendance and hours worked by each of the staff members was proving to be a challenge to the administrative department. A security measure is needed to keep safe designated areas in the outlet from unwanted visitors and to provide access to staff members only.

Subsequently, the company chose to use a fingerprint device over a proximity badge, favouring its distinctive features such as easy data management and effortless system implementation. The staff of Kinokuniya highly approved the TA102C, one of TimeTec Computing's FingerTec devices, remarking the ease of usage of the time attendance system and needing less time to clock in and out of work each day. Previously, the staff used a manual clock and this has resulted in issues such as long queues to punch in for work and cases of buddy punching. The system also ensures that only authorised personnel are allowed access to designated areas in the outlet, avoiding any breach in security.

Another retail company that has installed access control and time attendance systems is ARIANI. Established in early April 2008 with its first operational branch located in close proximity to one of the busiest business districts in Jalan Bunus, Kuala Lumpur, ARIANI is an exclusive scarf and headscarf brand that is owned by Ariani Textile & Manufacturing (M) Sdn Bhd. In the short span of five years, ARIANI has amassed a cult following amongst its faithful Muslimah customers which has led to the opening of 18 more branches nationwide to cater to the increasing demand for their high-quality products and the great customer service that forms the foundation of ARIANI's company mission and vision.

With the sudden boom in business and with the nationwide outlet expansion, trouble soon caught up with ARIANI when they realised that their old–school timekeeping system's manual work output calculation fails to prevent ever-increasing occurrences of human error and fraud. In a smart decision to move with the modern times and to muscle in their workplace management issues, ARIANI has of date installed a total of 17 FingerTec TA100C terminals in their Kota Bahru, Tanah Merah, Kuantan, Terengganu and Kubang Kerian outlets with more to come.

As the TA100C employs a systematic data collection method using Biometric fingerprint verification, attendance fraud or time theft problems are easily taken care of with just a swipe of a finger. Using the latest and most advanced algorithm in fingerprint verification, the TA100C simplifies time clocking while efficiently managing human resources to boost and facilitate employee punctuality and productivity.

Since the installation of the TA100C terminals, ARIANI is proud to report a steady decrement in buddy-punching and attendance fraud occurrences. The simplicity of the FingerTec TA100C series extends to its powerful TCMS V2 software where up to 1, 500 fingerprint templates and 100, 000 transaction instances can be exported from terminals to the software using a USB flash device for hassle-free viewing, handling, and generation of useful reports. Compliments were abound from ARIANI as the effective and reliable data management of the TA100C terminal combined with the TCMS V2 software has not only saved the time but also the resources of their HR department greatly.

Another prominent company in the retail industry that have benefited from having access control is Daiso, a large franchise of 100-yen shops in Japan, owned by Daiso Sangyo Corp, Japan. With a range of over 100, 000 goods, Daiso strives to develop and create a wide range of products as an essential part of their strategy to compete with high-end retailers.

With 2, 500 stores in Japan and 522 stores overseas including Malaysia, Daiso has managed to carve its name as the top choice for Malaysians when it comes to purchasing quality household items at RM5 per item.

As a growing organisation, Daiso acknowledges the importance of security and to help them solve their concern the company brought in experts to assess the security needs for Malaysia's HQ. FingerTec's R2 was recommended to be installed for Daiso's HQ due to its dual function, effective as a door access system and at the same time it works really well as time and attendance clock.

Investing in an access control and time attendance system is inevitable as it allows management the ability to monitor staff movement and generate reports based on the activities. With the Ingress software that is bundled with the device Daiso's management can view the real-time movements, detailed audit trails report, and can integrate the system with other security solution for a more holistic solution. All in all, Daiso is happy with the installation of R2 in the HQ, which leaves a possibility for similar system installations in other Daiso branches nationwide.

Conclusion

Finding the right security system for the retail industry means having one that can fit multiple functions. Access control is the primary form of security that prevents potential threats from entering the premise. Systems that are preventative are the best kind especially those with verification methods that utilises the latest technologies such as cloud and biometrics. Such verification methods are accurate and can be managed easily with the right kind of device and software.

Having a system that can provide workforce management functions will definitely be considered the best option, as it will reduce cost in purchasing systems as well as in their maintenance. It's a given that any company, and not only those in retail, can benefit from having an access control and time attendance system.

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

Hikvision Darkfighter Cameras Revolutionise Salford's Night-Time Surveillance

When Salford City Council began upgrading its public space CCTV cameras with Hikvision's Darkfighter models, video operatives reported some unusual results: they were suddenly able to see crystal clear night time images. Previously low-light surveillance images were murky and suspicious activity hard to make out. Now, armed with Darkfighter cameras from Hikvision, Salford's control centre is able to offer true 24/7 active monitoring while simultaneously reducing bandwidth requirements.

The City of Salford in England's northwest is a metropolitan borough of Greater Manchester, and includes Salford itself as well as the towns of Eccles, Swinton and Pendlebury, Walkden, and Irlam. More than 218,000 people live in the City, and Salford City Council and its partners fund 130 public space CCTV cameras, which cover eight neighbourhoods.

The CCTV cameras are monitored at a central control room located at Salford Civic Centre. This control room is linked to police radios so staffs are aware of incidents, missing people or people wanted for questioning, and can easily pass intelligence to the police. Information provided by the council's CCTV team helped police arrest 200 people last year.

In such densely populated urban environments, CCTV monitoring plays a crucial role, and not just for keeping an eye on unruly behaviour after pubs and nightclubs closes

for the evening. Salford City Council's cameras were key players in providing evidence for Operation Pandora, the Council's high profile crackdown on fly-tippers, illegally dumping rubbish in the City.

But previous cameras struggled to capture clear and effective public space video images in low-light scenarios. This meant that operatives found it hard to offer a true 24-hour monitoring service after 10pm or 11pm, depending on the time of year. Now that they have begun installing Hikvision's Darkfighter camera range, however, that is all changing.

An introduction to Hikvision2

Salford Principal Community Safety Officer Stephen Kearney said the Council began using Hikvision cameras two years ago after a house-building partner suggested using them to monitor a new development.

"I'd never heard of Hikvision and was not sure about using untried and untested cameras," he said. "So we did not install them at the development. We put them on the rooftop of one of our corporate buildings, and the next day the CCTV operatives called me and said you've got to see this – these are the best cameras we've got!

"So for the past two years we have not installed any cameras other than Hikvision, and in that time none of the Hikvision cameras have failed, which is not the case with the previous cameras we have used."

Challenges to overcome

Kearney said that as a local authority, Salford City Council faces multiple challenges when it comes to effective CCTV monitoring.

"The first of these is budget constraints," he said. "We don't have the luxury of being where we were five or more years ago when we had revenue funding available to support the growth of CCTV cameras, so we have to think extremely carefully about our ability to upgrade or replace our existing cameras when those go faulty. And the fact is that Hikvision's cameras are very competitively priced. "And because of the limitations of the cameras we had used before, we had struggled to provide a true 24 hour, 7 day a week service – just because they weren't able to capture low-light images of the quality that Hikvision's Darkfighter cameras can.

"In addition, the Hikvision cameras are far less bandwidth intensive than our older cameras. So we have a better quality product, it's cheaper to buy, and it's cheaper to actually run, because the bandwidth requirements are lower. So it's win-win all round. It's almost like an invest-to-save opportunity."

Enter the Darkfighters

After the initial use of two Darkfighter cameras as part of Operation Pandora's fly-tipping crackdown, Kearney approached his CCTV operators and asked where the most benefit would be gained from upgrading to Darkfighter cameras. As a result of their feedback, further PTZ domes were installed in October 2015 in Eccles Town Centre to replace older cameras.

The Darkfighter domes were supplied by distributor ezCCTV. The models used were DS-2DF8223I-AEL PTZ network domes. As well as their exemplary low-light performance, these domes have a 23x optical zoom Day/Night lens and feature a wide range of smart functions, including face detection, intrusion detection, line crossing detection and audio exception, are rated for tough outdoor use, and provide full HD1080p crisp video images.

Kearney said the results so far have been undeniably outstanding. "We tried the product, and its performance was unlike anything we had experienced previously. It turns night into day. As and when funding permits, we will definitely be replacing more cameras with Darkfighters. In an ideal world, we would swap out all 130 public space cameras for the new models from Hikvision!"

Future installations are planned to include Hikvision DS-2DF8336IV-AEL PTZ Darkfighter domes, which feature 36x optical zoom, and DS-2CD4A85-IZS 4K Ultra HD bullet cameras, offering ultra-high resolution images for powerful and effective real-time monitoring and evidential purposes.

Salford Deputy City Mayor Councillor David Lancaster said: "The CCTV cameras play a vital role in our city. Our staff reports incidents to police, enabling them to respond quickly, gather evidence for prosecuting fly-tippers and have saved dozens of vulnerable missing people by alerting the authorities. We were astonished at the clarity of the new 'Darkfighter' cameras. They really do turn night into day and give us pin sharp images, which will help immensely. Plus they are almost half the price of the previous cameras which is an additional bonus."

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

Hikvision Protects Striking New Islamabad Shopping Mall Development

Introduction

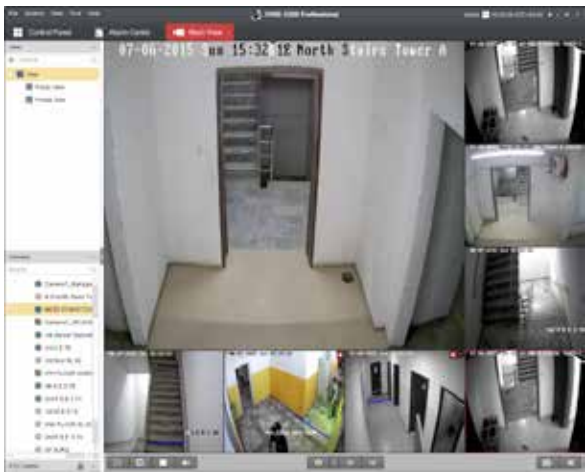
A building development can fairly be described as 'iconic' when it changes the very skyline of a city. That was the case in Islamabad, Pakistan, for Centaurus, a three-skyscraper complex - the tallest building in the city - all linked by a prestigious shopping mall. And, when the four-storey mall housing over 250 shops needed a powerful and effective surveillance system, they turned to Hikvision for high quality IP security video.

Centaurus is a mixed-use real estate development project designed by British architectural firm WS Atkins. The three 41-storey buildings house offices, a 5-star hotel, and residential apartments, with the luxury Centaurus mega mall running between and connecting the towers. The interior design of the residential building and the shopping mall was courtesy of renowned firm ODEION-Turkey. The striking complex was built at an estimated cost of US$350 million. All public spaces, particularly those that attract thousands of visitors every day, pose a security risk. As a major shopping hub, the Centaurus mall needs to be able to protect its customers and provide a safe and secure shopping environment.

Ensuring Customer Safety

The mall's management tasked Islamabad IP surveillance specialist installer, Digital Links, with providing a comprehensive video security system. The Centaurus security team was facing issues like garbage being thrown in stairways and emergency entry/exits. More seriously, security staffs were regularly receiving reports of thieves, shoplifters and pickpockets hiding in stairways to avoid detection. They would be detected once video was reviewed the following day - but by then, of course, it was too late. The new system had to monitor in real-time the key entry and exit points, the interior of the mall, and its emergency access points, as well as providing ongoing alarm monitoring. Hikvision's cameras were deployed to cover these crucial zones, as well as providing standard overall security views of malls and walkways.

Digital Links project manager, Khuram Chohan, says, "The solution we devised included 400 Hikvision DS-2CD2032-I 3MP Infrared IP Bullet Cameras and 80 DS-2CD2432F-IW 3MP IR Cube Network Cameras, which send video images back to eight 64-channel DS-9664NI-ST high-end NVRs. The whole system is managed using Hikvision's iVMS-5200 Professional Video Management Software."



Hikvision's iVMS-5200 Pro is a centralised video software management system that allows users to manage all of their business security subsystems in one platform. This single platform can control surveillance, access control, license plate recognition, business intelligence, and control room video wall.

Effective real-time monitoring

"The cameras plus the NVRs and the software provide a real-time live view for the Centaurus mall's security staff," says Chohan. "This enables them to monitor the mall effectively and efficiently. Powerful recording and remote playback mean video evidence is easily located and exported.

"The iVMS-5200 software provides a smart alarm handling mechanism which helps operators quickly locate and identify alarm incidents - and react quickly and decisively to prevent security incidents occurring.

"The system allows the entire mall to be monitored from the control room, where operators can proactively identify security risks. They are also able to ensure that emergency gates providing important access to the mall and skyscrapers are unobstructed and clear for emergency vehicles." The system's alarm functions, including motion detection, intrusion, video tampering and designated zone line crossing, have resulted in the apprehension of shoplifters and attempted thieves, and have solved the problem of unauthorised waste disposal in emergency exit staircases. The 480 IP surveillance cameras employed in the system send high resolution images to the control room for both live monitoring and recording - in order to investigate any incidents or suspicious activities. Operators are alerted to incidents via the iVMS-5200 Pro software's built-in video analytics capabilities, allowing resources to be immediately directed to any trouble spots.

The 64-channel DS-9664NI-ST network video recorders offer up to 6-megapixel resolution recording, and output at up to 1920 x 1080P resolution in HDMI and VGA formats. They provide up to eight SATA interfaces, dual gigabit network interfaces, and HDD quota and group management, which ensures long-time recording continuously without failure. The result is a shopping experience unlike any other in Pakistan, and a level of comprehensive security which is, for the mall's thousands of visitors, both reassuring and highly effective.

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

Sony Kicks Off Winning 4K Video Security Solution At Newcastle's Rugby World Cup Fanzone

Introduction

Fans all over the world have travelled to England for the Rugby World Cup 2015. As one of the host cities, Newcastle created a fanzone area as an extension to its stadium for spectators to watch and enjoy all of the matches, as well as get involved in lots of fun rugby-related activities.

When looking for a security solution to meet the demands of the busy site, Newcastle City Council made it clear that optimum image quality was a top priority in order to ensure the most effective monitoring possible. With a large area to cover, it was crucial that the solution would be able to capture the entire site and the minute details of the scene to provide round the clock surveillance.

Challenges

The site required a robust security solution, which offered broad coverage and the best footage quality. The solution needed to deliver all the benefits of the 4K technology, particularly high image resolution, without adding the strain on the video network. Newcastle City Council needed to cover a wide field view on the site whilst simultaneously having the ability to zoom in to areas of interest within the scene to make identification undisputable every time.

Sony solution

Sony's 4K SNC-VM772R security camera was installed to monitor the fanzone area. The 4K camera combines the enhanced resolution of up to 20MP with impressive low-light sensitivity, bandwidth optimisation features and intelligent scene capture capability (to automatically deliver the best picture quality depending on the scene), ideal for on-site surveillance at the Rugby World Cup fanzone.

Paul Angus, Community Safety Officer at Newcastle City Council explained, "When we were looking for a security solution on site, we wanted a top of the range product which delivered uncompromising image quality. Since installing the solution we have been very impressed with the enhanced image quality and wider scene capture. Compared to analogue and HD models, we've been able to see details within a scene much more clearly and can easily differentiate between colours and shapes in the images we capture."

Results

The fully integrated, easy-to-manage system has delivered comprehensive security at the fanzone during the Rugby World Cup. Traditionally, high-resolution imaging has come at the expense of low-light sensitivity. The high

sensitivity and 1.0 type 20MP Exmore R sensor used in the SNC-VM772R means that 4K high resolution recording is maintained regardless of lighting levels, enabling clear image capture in light and dark conditions. The implementation of 4K has created a streamlined security solution on the site, so identification can be accurate each and every time. The camera has seamlessly integrated within the site's large, existing security network, providing high image capture in the site's key area.

Why Sony was selected

Newcastle City Council tasked Universal Systems Solutions (USS) with providing detailed coverage of the entire site when it was at full capacity. The organisation entrusted USS to deliver the quality security solution it needed and thanks to the depth of USS's expertise and strong partnership with Sony, the company was able to seamlessly fulfill its customer's requirements. This was achieved by implementing a reliable solution, which fitted with the existing Sony models, providing 4K-image coverage in the required area at a low bandwidth.

Conclusion

Kevin Bruce, Director at USS says of the solution: "Having worked with Sony for many years, we remain impressed by the breadth and quality of its video security solutions which meet the high standards of our customers. The combination of the 4K camera's lower bandwidth, night time viewing and back light compensation made it the ideal option for Newcastle City Council's fanzone. Sony's technology has been core to delivering against the brief and migrating to the latest future-proofed surveillance system for this project."

USS was impressed with the SNC-VM772R's hassle-free fitting and ease of installation on site. The SNC toolbox mobile, a convenient app that provides a simpler and smarter video security camera setup for installers, meant the camera could be easily installed at a very high point and managed via a smartphone, omitting the need for the installers to climb up and down ladders to adjust the field of view.

For more information, please visit: http://pro.sony-asia.com/pro/lang/en/hk/products/video-security SST

Physical Identity Access Management Systems Prescribed For Hospital Safety And Security Wellness

Article Attributed to Ajay Jain
President and CEO of Quantum Secure

Introduction

The rise in violent incidents sweeping throughout the world has organisations across all industries looking for new and more effective ways to control access in order to better protect and secure people and the premises they are in. One of the areas most affected by these incidents is the healthcare industry.

Impact on hospital operations

Hospitals and clinics face regular threats to people and property from outside sources as well as from within. Physical assaults, theft of medical supplies or equipment that contains confidential patient information, and even infant abductions are all issues that today's healthcare administrations must contend with.

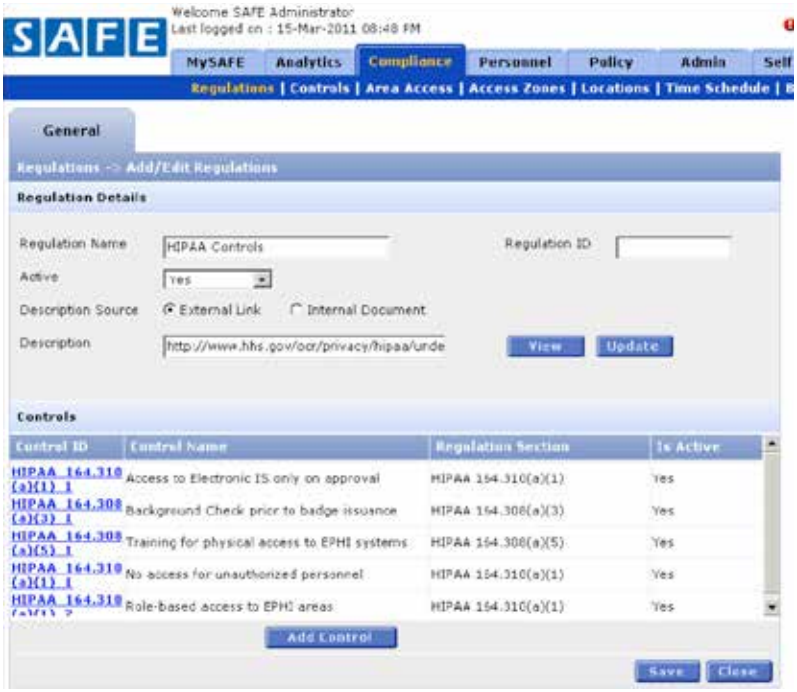
Two additional developments in the healthcare industry have made the situation even more acute. The first is the advent of the Affordable Care Act (ACA), which has the potential to substantially increase the number and frequency of patients and visitors to what may be a growing number of healthcare facilities. These increased numbers will in turn require strong and more enforceable access restrictions. The catch-22 is that hospitals, medical research centres and so on, not unlike school campuses, are semi-public facilities. Administrators want to maintain an atmosphere of friendliness that allows medical staff, visitors or contract workers to go about their business with relative ease. This openness must be balanced with the facility's obligation to maintain a safe and secure environment for all.

The ACA could initially also create a situation for healthcare facilities that results in system overload and cost overruns. For example, if professional guard services are reduced, the reduction in trained manpower could potentially result in less scrutiny of hospital visitors or longer action times in the event of an incident. In another example, hospital workers may be overburdened with additional paperwork required by the ACA, and not immediately notice that a patient has gone missing or that individuals are tailgating to enter restricted areas. These are real challenges facing today's healthcare facilities.

The second development is the trend toward removing restrictions on hospital visiting hours for family and friends. Recent reports indicate that allowing patients to spend more time with family and friends can improve outcomes by lowering patient anxiety levels and feelings of social isolation. Studies also suggest that individuals recovering from surgery that have family with them suffer less nerve-related pain and their inflammation levels lower faster.

While this trend of relaxed visiting hours is proving beneficial to the health and recovery of patients, it places an additional security burden on hospital administration. Policies and procedures must be developed and implemented that will allow a more open environment but will protect the privacy of other patients, and the safety of patients and staff. Policies must also take into account procedures for emergency situations such as a lock-down or evacuation. Knowing exactly who is in the facility and why they are there is valuable information at any time and under any circumstance.

Automated solutions are key



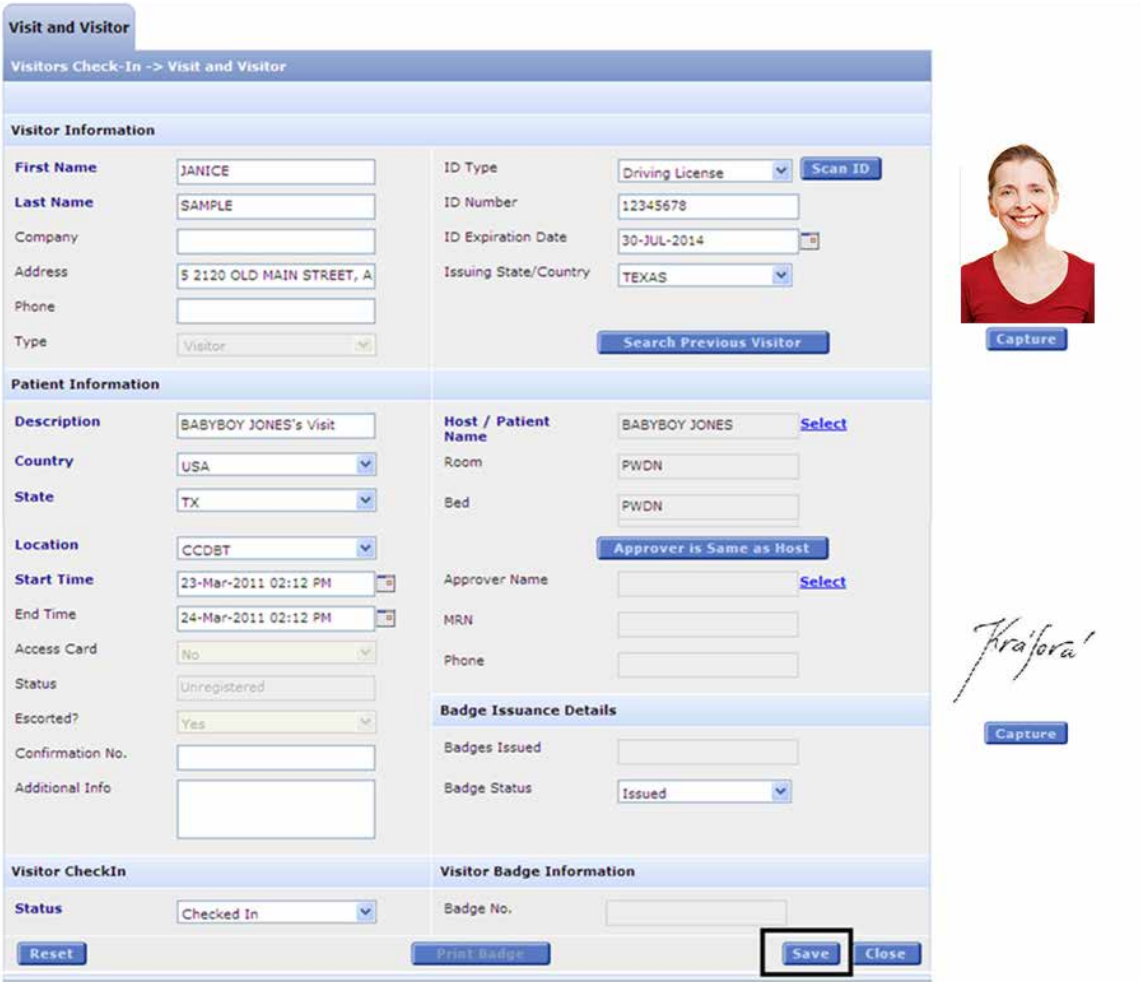
Credentials such as visitor passes and access cards physical access but the true issue is the management thereof. Requiring visitors or contractors to manually sign in and out, or wear a visitor badge is difficult if not, near impossible procedure to enforce. Employee badging systems help identify those authorised to be in the hospital but in some cases, badges can be easily forged, and if the badging system is not integrated with other hospital security systems they are significantly less effective as an access control solution.

For safety's sake, everyone coming in and going out of a healthcare facility should be easily identified and have controls placed on their access. A proven solution to help mitigate the overall effect of a more open healthcare environment and lessen the potential for security breaches is the

use of intelligent and purpose-built automated physical identity and access management (PIAM) software. A ready-made solution for healthcare organisations, PIAM solutions allow administrations to upgrade and enhance their physical security strategies to meet the challenges of the Affordable Care Act, and accommodate new trends while remaining compliant with requirements mandated by various healthcare regulations.

With a centralised PIAM system, a healthcare organisation can create an identity for every individual who has reason to be on the premises. By connecting diverse existing physical security, IT and other systems, PIAM solutions can automate key processes and workflows to optimise security operations, centralise control, and enable compliance with regulatory mandates to be automated in real time.

Software systems can streamline time-consuming and inefficient processes from issuing ID badges to managing databases to assigning access privileges across multiple physical access control systems. For instance, when a hospital is affiliated with or physically part of a University School of Medicine, various access levels and permissions can be programmed on to a single ID badge for physicians and students. In addition, any activity, event or status at any point in the identity lifecycle is reportable and auditable. If vulnerability is identified, hospital administrators can review and take the necessary action to rectify procedures or activities.



Managed control to meet compliance

The Joint Commission for the Accreditation of Healthcare Organisations (JCAHO) oversees the industry's accreditation process to ensure patient/personnel safety and standards compliance. Among other stipulations, accreditation requires that healthcare facilities identify sensitive security locations within the hospital (i.e. birthing centres, pharmacy, emergency, etc.) that may require unique security protection. Hospitals without controlled access rights to sensitive areas are at risk of losing accreditation, along with funding. Further, the Centres for Medicare and Medicaid Services (CMS) conduct their own inspections, the results of which can affect the facility's accreditation.

Adherence to rules and regulations established by state and federal agencies is not only mandatory but it also meets best practices with regard to hospital safety. Compliance with regulatory mandates is an important element of risk management and PIAM software can enable these initiatives to be automated in real time. As an example, HL7 refers to specific standards for the exchange, integration, sharing and retrieval of electronic health information. When PIAM software is integrated with a patient's electronic health record (EHR), the combined information provides a more holistic view for the medical professional. All information pertaining to patient identity, such as visitors, dietary restrictions, medical attendees and so on, are tied together under policy-based workflows.

Conclusion: The need for change

Hospitals and other healthcare facilities need good access control and visitor management to maintain an open and safe haven environment. PIAM software is a holistic approach to managing access that helps ensure that each identity has the right access, to the right areas, for the right length of time. The benefits are many and ultimately provide healthcare facilities with the tools to address access control and visitor management in today's security conscious environment.

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

IN FOCUS

SECURITY DEMANDS FOR EMERGING MARKETS IN ASEAN

Article attributed to:
Riki Nishimura
General Manager of Visual Security Solutions Division, Professional Solutions Company (PSAP) at Sony Electrics Asia Pacific

Introduction

With the opening of local economies, emerging markets in the ASEAN region are experiencing an influx of foreign investments coupled with new infrastructure developments. The fast-paced growth also increases security demands, with government placing more emphasis on the implementation of physical security systems and solutions in order to secure the premises, assets and its people. As a thought leading in the security and surveillance arena, Sony sees the tremendous potential of growing this business across the ASEAN region.

"Sony's reputation as the industry-leading technology innovator, solutions provider and trusted business partner showcases our offering goes beyond the dated vendor/customer practice. We concentrate on building relationships that empower our partners and customers," said Mr. Riki Nishimura, General Manager of Visual Security Solutions Division, Professional Solutions Company (PSAP) at Sony Electronics Asia Pacific. "With the whole gamut of video

security products, we are confident in providing solutions that cater to specific needs of our clients and ensure that it will be an effortless process for them. For example, Sony's latest 4K video security camera (SNC-VM772R) aims to address the concerns of our business partners to achieve both high resolution and high sensitivity while battling the increased system costs."

Government as a core driving force

Mr. Nishimura observed that the core driving force in these emerging markets would be government bodies followed by the banking/financial and retail sectors. "Increasingly, financial institutions are enhancing their surveillance systems to meet security, regulatory and compliance demands, while addressing their concerns for efficiency and productivity. On the other hand, retail market is also booming with the opening of more high-end boutiques which require higher security requirements."

He also remarked that the hospitality sector could be one of the new opportunities for the security industry. "Tourism is a huge economic driving force for these emerging markets. With the rising numbers of hotels and entertainment establishments, we foresee that this will generate demands for security and surveillance solutions."

Challenges in the distribution market

Mr. Nishimura highlighted the possible challenges in the distribution markets of these countries especially for new foreign players. Apart from cultural taboos as well as

possible language barrier, finding the 'right' local partner would be the key to effective market penetration. These 'right' partners will be able to facilitate and expedite market entry with their in-depth knowledge and established networks and assist new players to establish a foothold within the market.

In addition, there may be limits on new players through licensing requirements, restricted access to raw materials, product testing regulations, among other constraints. Nonetheless, Mr. Nishimura remained positive and stressed the importance of understanding the regulatory framework within these markets. "It is important that products meet the local standards apart from the global ones. This will definitely boost consumer confidence and reputation of the company in the long run."

Looking ahead

Apart from immediate installation demands driving these emerging markets compared to other more developed regions, Mr. Nishimura commented that 4K imaging will soon be a global video security standard. "It is more than just increased resolution. It is expanding the application potential of security cameras and helping to transform security and surveillance. For example, the SNC-VM772R has received overwhelming responses across Europe and the product promises to be a real game changer for the market as customers unlock the true value of 4K imaging."

For more information, please visit:
http://pro.sony-asia.com/pro/lang/en/hk/products/video-security SST

BOSCH
Invented for life

Making Professional Video Surveillance Easy For Everyone With The DINION IP Bullet Cameras

Obtrusive design for obvious outdoor surveillance

The highly visible, dust and watertight (IP66) DINION IP bullet cameras are great for outdoor use in elevated locations like high up on a wall where first-time-right installation is particularly important. They offer a 720p or 1080p HD resolution for detailed images to easily distinguish individuals or minor details. Built-in infrared illumination enables object detection at a distance of up to 30 metres even at night.

Simple installation

Considering its usage situation the common challenges when installing a bullet camera are cable management and ensuring a dust and watertight connection. DINION IP bullet cameras can therefore be delivered with a dedicated surface mount box. This provides a hook to connect the camera to the mounting box, so installers can focus on connecting the cables without holding the camera.

Safe data storage

DINION IP bullet 4000 and DINION IP bullet 5000 cameras provide an easy back-up solution. Video data can be safely stored in the cloud, on a network video recorder, or on a built-in SD card. Any of these methods provide an easy back-up solution to safely store relevant video data.

24/7 remote access and camera control

All DINION IP bullet cameras are fully supported by Dynamic Transcoding technology. It gives users easy 24/7 remote access to camera controls, live video streams, recordings and multi-megapixel images. To gain all these benefits, simply expand the IP video surveillance system with a Bosch recording solution like the DIVAR IP series or VIDEOJET XTC XF.

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

The RFID-Based EAS Overhead 2.0 Solution

Checkpoint has raised the bar for operational excellence by introducing the next generation in integrated merchandise visibility and loss prevention: the RFID-Based EAS Overhead 2.0 Solution.

This new solution delivers a new dimension – literally – in RFID-based merchandise availability with an integrated solution that is smaller, more flexible, easier to deploy and able to deliver better performance than previous overhead solutions. Overhead 2.0 serves as an EAS system that alarms and identifies stolen merchandise, improving operations at the point-of-exit while enhancing the customer shopping experience by helping to ensure merchandise availability, giving retailers unprecedented confidence and flexibility in optimizing their stores for intelligent merchandise availability. Supports wide and high entrances

- Small, modular design
- Improved performance
- Better aesthetics
- Enhanced front-of-store merchandising
- Supports the newest, most functional RFID tags on the market
- Easier to deploy

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

Compact, Cost-Effective And Flexible HDTV Surveillance With WDR

With features such as Lightfinder and WDR – Forensic Capture, the bullet-style AXIS P1435-E provides excellent image quality in HDTV 1080p resolution, even in complex light conditions. In addition, the camera supports Axis' Corridor Format, pixel counter, remote zoom and focus, as well as P-Iris control. The day and night camera is ideal for 24/7 video surveillance, in exposed outdoor areas such as parking lots and service stations, and for general indoor surveillance purposes wherever a compact camera is needed.

Excellent image quality

AXIS P1435-E with its varifocal, P-Iris lens provides excellent image quality at up to 60 frames per second. P-Iris control provides optimal depth of field, resolution, image contrast and clarity.

Lightfinder and Wide Dynamic Range (WDR)

With Wide Dynamic Range – Forensic Capture, the camera provides perfectly balanced video quality in scenes with strong variations in light, while Axis' Lightfinder technology enables outstanding image usability in poor light. The camera can seamlessly transition between handling WDR and low-light conditions.

Edge storage and Zipstream

AXIS P1435-E offers support for edge storage that makes it possible to record video directly to a storage such as a microSD/SDHC card, thereby creating a flexible and reliable video surveillance system. In addition, Axis' Zipstream technology lowers bandwidth and storage requirements by an average of 50 per cent without costly and complicated integration. Zipstream ensures that important details in the image get enough attention in the video stream while unnecessary data can be removed.

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

MicroEngine®
Integrated Security Systems

MicroEngine's Encrypted IP Desfire Controller – GLS300

GLS 300 is a multifunctional single door controller that supports the latest Mifare contactless technologies – Mifare DesFire EV1. Through the implementation of Mifare DesFire, GLS300 offers the highest security measure in access control system such as the data communication from start to finish is encrypted using the very secure algorithms of Triple Des (3DES), 3KDES & AES.

It provides the highest security control in access control system as it supports the RFID chips with UID up to 64 bits or 20 digits. Hence, it can countermeasure the security risk relating to duplicate card ID.

It is equipped with LAN connectivity at 10/100 Base-T using TCP/IP protocol. The messaging between the GLS300 and software is encrypted with dynamic key using AES128 industrial strength algorithm.

GLS300 has built for high-end integrated security applications by using the 32 bit RISC processor at 80 MHz for industrial application and it enables the system to process complex applications such as modern security encryption features in real time manner.

It can support door access control, car park access control and lift access control. Users can configure the capacity of system by adding extension boards.

It supports our in-house PLATO Desfire readers on RS485 connection which offer user the option of multiple mode of reader only, reader + keypad + colour LCD operations. Thus, the door can be configured to operate on different entry access mode at any time.

It has 4 supervised inputs, 1 for exit button, and 1 for door sensor. The other 2 are for general purpose Inputs that can be used as Alarm sensor input. It also has built in DEDICATED Tamper Switch Input and Fire Alarm Input for higher standard requirement.

In addition, it provides 2 Weigand / ABA reader input that support 64bit card number.
GLS300 can store up to 100,000-card user database and 50,000 transaction records.

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

Model: Industrial Video Encoder VPort 461A

By: Moxa Inc.
ⓘ www.moxa.com

- Supports up to 3 video streams simultaneously for H.264 and MJPEG
- Up to Full D1 resolution (720 x 480) @ 90 FPS for 3 video streams with legacy analog video images
- Video latency under 200 ms
- 2 Ethernet ports for cascade and Ethernet port redundancy
- Moxa DynaStream function supported for network efficiency
- ONVIF supported for standardization and interoperability
- Local storage capability with SD card slot
- Industrial design with -40 to 75 degree celsius operating temperature

Model: OSD2153P

By: Optical Systems Design Pty Ltd
ⓘ www.osd.com.au

- Industrial PoE+ Gigabit Ethernet Media Converter
- DIN-Rail or wall mountable
- Supports IEEE 802.3af and 802.3at PoE
- Supports Link Loss Forwarding
- Extremely small and robust module
- Operates over the temperature range of -20 to +75 degree Celsius

Model: WMB-300Ap V6

By: Brickcom Corporation
ⓘ www.brickcom.com/

- Support 802.11a/b/g/n Dual Band Wireless Connectivity
- WPS Supported for Easy Wireless Network Setup
- Built-in IR Illuminators up to 15 Metres
- Removable IR-cut Filter /Auto Light Sensor for Day and Night Function
- Built-in Micro SD / SDHC / SDXC Memory Card Slot for Local Storage
- Two-way Audio / Built-in Mic and Speaker / 1 DI/DO for External Alarm and Sensor Device / PIR
- Wide Angle view with Board Lens
- i-Mode for Different Environments

Model: Symmetry CompleteView Video Management System

By: AMAG Technology
ⓘ www.amag.com

- Per-camera configuration of all video streaming and recording parameters
- Advanced PTZ control on event, live/recorded video
- Simultaneous support for multiple video formats
- One time, per camera license fee – no server or client fees
- Dynamic Resolution Scaling reduces bandwidth consumption
- Smart Search – quickly find event based on motion in a defined area
- Thumbnail Search capability
- Support for IP cameras and encoders by leading manufacturers

Model: DINION IP bullet 4000/5000 HD

By: Bosch
ⓘ www.bosch.com

- Easy to install with auto zoom/focus lens, wizard and pre-configured modes
- Built-in IR illuminator with 30 m (98 ft) viewing distance
- Automatic Varifocal (AVF) to save time when focusing individual cameras
- Regions of interest and E-PTZ
- True day/night switching to maintain sharp focus under all lighting conditions
- IP66 surface mount box
- Offers in 720p or 1080p resolution for sharp images

Model: AXIS Q6128-E PTZ Dome Network Camera

By: Axis Communications
ⓘ www.axis.com

- 4K resolution at 30 frames per second
- 12x optical zoom and autofocus
- Quick and precise pan of up to 700 degrees per second
- Offers Electronic Image Stabilisation, giving smoother video in windy conditions
- Features defogging and is protected by shock detection that sends an alarm if someone tries to vandalise it
- The built-in video analytics of AXIS Q6128-E includes Advanced Gatekeeper that allows the camera to detect an object in a specified area and zoom in on it
- Designed for reliable, weather-proof installation with built-in protection against dust, strong water jets, rain, snow and sunlight (IP66 and NEMA 4X rating), and impact resistance (IK08 rating)

Model: "FirstLane" (security turnstiles)

By: Automatic Systems
ⓘ www.automatic-systems.com

- Best in class for electronic detection
- Modern and stylish look
- Low energy consumption for a low carbon footprint
- TCP/IP communication
- Fast opening/closing of swing doors (< 1 sec.)
- Dynamic, electronic user protection
- Easy to install
- Electro-mechanical drive units

Model: P2000 Security Management System Version 3.14

By: Johnson Controls, Inc.
ⓘ www.johnsoncontrols.com

- Interactive, real-time, 24/7 security management
- Open platform system supporting hardware from multiple manufacturers
- Integrates with multiple third-party systems such as human resource, building automation, intrusion and video with available APIs for customised solutions
- Easy to use with intuitive graphical user interface
- New advanced web user interface and mobile applications allow many operations to be completed from a web browser or Android and iOS mobile device
- Advanced web-based situational awareness features including real-world geo-located maps, alarm manager
- Mobile features include alarm management, door control and cardholder activity view

Model: ALGATEC 600lbs Single Series EM Lock: UL275-SL-A

By: UWC Electric (M) Sdn Bhd
ⓘ www.uwcelectric.com

- Designed to meet fire and life safety applications
- Integrated Lock Status Monitoring feature (LSMF) – Monitored type with build-in bond sensor
- Fail Safe
- Zero Residual Magnetism
- Dual Voltage Input, 12Vdc or 24Vdc selectable
- Ease of installation with low maintenance & low energy consumption made it become a cost saving product
- This EM Lock operate quietly & care free

Model: PK-UHF201

By: Pongee Industries Co., Ltd.
ⓘ www.pongee.com.tw

- Protocol comply with UHF EPC Gen2 (ISO18000-6C), ISO 18000-6B standard
- Support adjustable frequency range (FHSS) or fixed specific working frequency
- Power output 0 – 30 dBm (adjustable)
- Built-in 8dBi/12dBi polarised antenna as choice
- Reading range 3~5M / 10M
- Support operation Modes as Answer, Active, Trigger mode
- Low power design, Input Power: DC +9V
- Support RS-232, RS-485

Model: OSDP Networked Controller (AC-825IP)

By: Rosslare Enterprises Ltd
ⓘ www.rosslaresecurity.com

- 4-door (In/Out) networked access controller
- Backbone of medium to high-scale security system
- One onboard expansion slot – further 12-board expansion via OSDP
- Driven by AxTraxNG – powerful, flexible, and easy-to-use software (FOC 64 panels)
- Modular/expandable solution up to 58 doors per panel
- Perfect for commercial and enterprise applications
- AES 128-bit encrypted TCP/IP communication to AxTraxNG server

Model: MorphoAccess SIGMA Lite Series

By: Morpho
ⓘ www.morpho.com

- Slim and powerful fingerprint access terminals
- 1:10,000 user identification in 1 second
- High capacity: 30,000 templates, 250,000 IDs in authorised user list, 1 Million logs
- Anti-fraud features: fake finger detection, duress finger, timed anti-pass back
- Flexibility: Prox, iClass or MIFARE/ DESFire/NFC contactless card reader as an option
- Embedded web server
- Tough design: weather (IP65) and vandal (IK08) resistant
- Compatible with Morpho and Bioscrypt existing installations

Model: Checkpoint Attack Spider Wrap

By: Checkpoint Systems, Inc.
ⓘ www.CheckpointSystems.com

- Available in both 2 and 3 Alarm
- 70 inches and 102 inches length, 7- strand aircraft grade cable for maximum protection
- Tough, secure and reusable
- Protected speaker minimises defeat and produces a 96 dBA alarm—4 times louder than competitive products
- Internal clutch and easy-wind flip top creates a more secure fit
- Red flashing LED and speaker grill create a strong visual deterrent
- Auto-lock feature reduces the number of steps required to apply
- Lithium battery provides years of hassle-free operation

Model: VeriFire

By: GKB Security
ⓘ www.gkbsecurity.com

- Early-stage fire & smoke detection and notification
- Customised interfaces: VeriFire open API interface with the 3rd party specialist developers in mind
- Onvif IP-based expandability: easy to integrate with Onvif third party VMS
- 1080P CMOS Megapixel Sensor
- Two-way audio
- DI/DO
- 4 video streams
- ROI

Model: SISMA CA

By: DEA Security S.r.l.
ⓘ www.deasecurity.com

- Invisible - Placed on the surface of the slab and drowned in the screed, SISMA CA sensors are totally invisible
- Accurate - SISMA CA allows you to accurately locate the area concerned by the intrusion and identify the single access under alarm
- Maintenance free. Thanks to their particular technology, the sensors do not need any planned maintenance
- Immune to environmental nuisances - the system is not affected by adverse climatic events (snow and hail including) and by the falling of leaves or small boughs
- Sensitive - even though it is installed under a thick layer of concrete and it is designed to resist loads of tons, SISMA CA sensors can perceive the slightest step
- Intelligent - the system can discriminate the passing of small animals from real intrusions
- Quick to install - SISMA CA sensors are provided in prewired modules, while the electronic boards are preassembled in special polyester cabinets.

Model: NV35M

By: Paradox Security Systems
ⓘ www.paradox.com

- Outdoor/ indoor protection solution for windows and sliding doors
- Ultra low power management operation with Paradox Effi+ circuit
- Dual tamper detection (removal of cover or unit)
- Increased white light rejection
- Digital EMI / RFI interference rejection
- Optical Pet discrimination geometry to support super Pet Immunity
- Dual detectors, managed by Full Authority Digital Electronics Control (FADEC)
- Patented Auto Pulse Signal Processing with Automatic Temperature Compensation
- Anti-masking: Unique active IR detection for both blocking items up to 30cm in front of the detector and sprayed liquids

Model: INTREPID Model 336 Long Range Digital Microwave Link

By: Southwest Microwave, Inc.
ⓘ www.southwestmicrowave.com

- Range: 457 M (1500FT)
- Rugged construction for reliability against mechanical abuse and harsh climatic extremes
- Embedded digital signal processing (DSP) for High PD/ Low NAR
- Software-controlled setup
- Low power consumption
- Monitoring via on board form-C relay alarm outputs
- Advanced EMI/RFI shielding and surge protection

Model: KX wireless detectors

By: Pyronix Limited
www.pyronix.com

- Easy installation with one-push-to-learn and signal strength indicator features
- Using the same housings throughout the wireless and wired KX range ensures aesthetic consistency for a slick look and finish
- The KX's can fit onto any Enforcer panel from our range, as well as our PCX panel using a PCX32-WE
- Whatever the installation, the KX wireless range of detectors can cater for any need, with pet immunity, dual-technology, long-range curtain and PIR coverages available.
- Digital Temperature Compensation allows the detectors to automatically adjust to maintain detection range in hot and humid environments
- The KX range utilise our patented independent floating thresholds (IFT). All electronic devices cause electrical interference, from mains power to computers.
- All KX's in the range provide Grade 2 level security

Model: Control Panel Eclipse 32

By: Teletek Electronics JSC
www.teletek-electronics.com

- Up to 32 zones with freely programmable parameters
- 8 independent areas (partitions) with individual programming.
- Flexible programming via keyboard or ProsTE software.
- Available firmware update
- 3 different programming modes
- Up to 30 devices connected to the system bus
- Wide range of detectors, periphery devices and communication modules

Model: Pearl Triple-Tech External Detector

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

- The Pearl uses Triple technology including PIR, microwave and anti-masking
- Up to 12 metres selectable detection range (3m, 6m, 9m, 12m)
- Utilises masking detection to prevent intruder tampering
- Robust IP65 housing
- Narrow PIR curtain lens
- Protects windows, doors or full lengths of a building
- Two year warranty

Model: VarioCAM HD head

By: InfraTec GmbH Infrarotsensorik und Messtechnik
ⓘ http://www.infratec-infrared.com/

- Uncooled detector with (1,024 x 768) IR pixels
- Optomechanical MicroScan with (2,048 x 1,536) IR pixels
- Spectral range (7.5 to 14) m
- Personnel detection range 6.1 km
- Vehicle detection range 10.7 km
- Solid light metal housing (IP67)
- Quality from Germany

Model: IP Controller, IPC Series

By: MARSS IP & Security srl
ⓘ www.marss.eu

- An innovative system of stand-alone TCP/IP modules that allow the remote and intelligent management of any installed device/system by smartphones or tables via APP IP controller and by PC via webserver
- Via the APP "IP Controller" the end users can make different domotic functions, exploiting the existing installations
- APP free-downloadable for iOS and Android with GUI interface - users can customise icons and labels
- Equipped with the MARSS Cloud Technology
- Advanced functions (inter-connectivity of more modules; matrix functions) and high level of Security
- Centralisation software up to 1000 IP Controller Modules

Model: CW-400NAC

By: Cerio Corporation
ⓘ www.cerio.com.tw

- Utilises an 800mW High Power 1200AC Dual-Band Ceiling/Wall Mount Design
- Supports 2.4GHz Transmission Rates of up to 300Mbps
- Supports 5GHz Transmission Rates of up to 867Mbps
- Integrates PoE Bridge function to power subsequent devices (IP Cameras) through Ethernet connection
- Supports 802.11ac/n/an/a wireless standards
- Utilises both IEEE 802.3af/at Power over Ethernet and DC Power input
- Reliably supports up to 100 concurrent wireless clients
- Integrates smart Band Steering technology

Model: Espresso

By: Matica Technologies Group
ⓘ www.maticatech.com

- Compact and powerful Direct-to-Card printer
- Monochrome print speed up to 850cph or full color up to 210cph
- Single side or dual side printing
- Optional WiFi and Ethernet connectivity
- Encoding options including magnetic stripe, contact / contactless smart card
- Applications / Markets: corporate ID, membership badges, gift and loyalty cards, etc

Model: Netwave Wireless

By: ComNet
ⓘ www.comnet.net

- Consists of an easy to install, pre-packaged Point-to-Point kit to establish remote connectivity to Ethernet edge devices
- Also available are Point-to-Multipoint models for multiple connections
- NetWave will support a throughput of up to 500 Mbps which are PoE compliant and temperature hardened
- Meets class IP67 dust and water ingress protection standards
- Now NetWave models are available in a small size unit for space constrained installations
- Lifetime Warranty
- Designed by ComNet In USA and hand assembled in UK

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

COSELEC
A deister electronic GmbH Company

- RFID Electronic Key Management System
- Guard Tour System
- Vehicle Access Control System
- Contactless Smartcard System
- Biometrics Verification System
- Multi - Technology Card Reader

deister electronic
The RFID Company

WE THINK SECURITY
Blk 28 Kallang Place #06-12/14
Singapore 339158
Tel: (65) 6741 5200
Fax: (65) 6741 6200
RCB No: 19880111W
Email: info@coselec.com.sg
www.coselec.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

Southeast Asia **building**
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.

• SOUTHEAST • ASIA •
CONSTRUCTION

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

Secutech 2016 Highlights Next-Generation Intelligent Solutions In Home Security

Secutech will return from 19 – 21 April 2016 at the Taipei Nangang Exhibition Centre in Taiwan. Entering its 19th edition, the fair will span 35, 873 square metres of exhibition space and house around 500 exhibitors from 17 countries and regions.

Commenting on the show's development, Regina Tsai, Deputy General Manager of the organising committee said, "Home security is expected to remain one of the strongest sectors within the entire security industry in the next 5 to 10 years. Understanding the growing demand for connected home systems and devices across the region, we are organising SMAhome Expo – a dedicated zone for the smart home industry – again at Secutech 2016 to assist buyers in sourcing from suppliers of key components and advanced technologies, such as IoT, cloud services and HEM (Home Energy Management) systems."

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

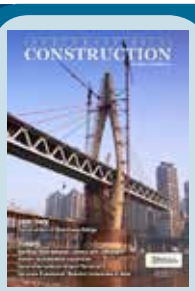
Bathroom + Kitchen Today

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

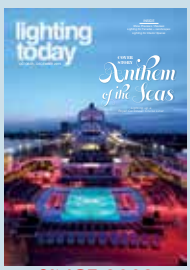


SINCE 1994

☐ 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: _____

To date, over 150 leading manufacturers from China, Korea and Taiwan have already signed up for SMAhome Expo. Significant brands include ASUS, Amroad, GKB, Heiman, SecuFirst, Sunmore , TrendMicro, StarCam and Unitech.

Tsai added, "We are anticipating over 26, 000 system integrators, dealers and distributors and industry professionals to visit the fair. With the range and high quality of participating exhibitors on offer, I am confident that visitors will not only discover a wealth of solutions and products but will also find ample opportunities to establish new and invaluable industry partnerships."

Concurrent events facilitate information exchange and offer ample networking opportunities

Held alongside Secutech 2016, a series of complementary activities will play a crucial role in unveiling the latest trends, while also enriching participants' experiences at the fair.

Amid this programme, the Smart Home M2M (machine-to-machine) Platform & Software Summit will be held for the first time to foster knowledge flow and promote cooperation between smart home software/platform designers and hardware manufacturers. The speaker line up is comprised of open source IoT projects specialists, connected device platform suppliers; smart home software stacks developers, cloud-based video solution providers as well as other application software designers. They will present and discuss industry hot topics such as connectivity, interoperability, data protection and business models.

Another event highlight is the Smart Home Protocol Gallery. It showcases the newest applications of Z-wave and ZigBee international standards on home automation, collaborating with premium manufacturers offering distinctive product design and comprehensive technical support.

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

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 british security industry association

NSI Security.Improved

ASIS INTERNATIONAL EUROPE

IPSA

Organised by

UBM