

NOV / DEC 2019

SECURITY SOLUTIONS TODAY

KEEPING EVENTS SAFE

Ensuring security frameworks are in place during an emergency.

SECURITY

In Focus

Facial Recognition Technology And The Threat To Privacy Rights

In Focus

Security Concerns For Biometric Data

Healthcare Feature

The Safety Net Formed By Connected Tech

Residential Feature

Consumer Responsibility In IoT Security

NVR 4.0

New UI, New Experience

Redesign for easy to use



- No plugins in web browser improving the compatibility of different web browsers
- Support cross-day-search to realize easier target search
- Hard disk format notification to avoid loss of important data
- Better compatibility with TPC, AI fisheye, PTZ cameras, etc.
- Newly added firewalls and network security protocol to secure the system
- Seagate* SHM (SkyHwak Health Management) actively protects the data

Recommended Models



NVR2000-4KS2



NVR4000-4KS2



NVR5000-4KS2



NVR4000-I



NVR5000-I

CE FC CCC UL RoHS ISO 9001:2000



SKYHAWK
HEALTH

SkyHawk Health Management (SHM) is drive health monitoring software co-developed in cooperation with Seagate.



DAHUA TECHNOLOGY SINGAPORE PTE. LTD.

Add: 62 Ubi Road 1 #06 -15 Oxley Biz Hub 2 Singapore 408734

Tel: + 65 6538 0952

Email: sales.sg@dahuatech.com

Facebook: @DahuaTechnologySpore



Safety & Security Asia 2019

The 18TH International Safety & Security Technology & Equipment Exhibition

1 - 3 October 2019

Halls B & C, Marina Bay Sands, Singapore

10,000sqm gross exhibition space • **250 exhibitors** from 20 countries •
9,000 trade professionals from 40 countries

*Combined statistics across Architecture & Building Services 2019

Be a part of **Safety & Security Asia 2019** - the quality sourcing platform for excellent commercial security solutions. Showcase your latest technologies, innovations and related services in the safety and security arena in the most established and longest-running commercial security tradeshow in ASEAN!

JOIN SSA 2019 TODAY AND

Expand your business network and explore new opportunities
Stay updated on industry trends and developments
Maximise your marketing & publicity efforts

For booth enquiries, contact:

SSA@cems.com.sg or call
(65) 6278 8666

www.safetysecurityasia.com.sg

A Part Of



Architecture & Building Services 2019
Providing Solutions for
Smart Nation Building

Organised By **CEMS**
Conference & Exhibition
Management Services Pte. Ltd.

1 Maritime Square #09-43, HarbourFront Centre, Singapore 099253
info@cems.com.sg • (65) 6278 8666

IN THIS ISSUE

6 Calendar Of Events

8 Editor's Note

10 In The News

Updates from Asia and Beyond

24 Cover Story

The Ins And Outs Of Event Security

30 Security Feature

- + IoT And Home Automation: What Does The Future Hold?
- + Securing Consumer IoT Devices: Why A Global Standard Is Needed
- + Security Challenges For The Future Of IoT
- + Mobile Apps: Insecure By Default
- + Giving Consumers Responsibility In IoT Security Regulation
- + Game-changers For Smart Residences
- + IoT Healthcare Sensor Revenues Grow Globally
- + How To Protect Yourself From The Siren Song Of Healthcare IoT
- + How Smart Cities Improve Accessibility For The Elderly
- + Project UFOund: Improving Hospital Logistics With IoT
- + 3 Ways Video Technology Can Improve Patient Safety In Healthcare
- + As Food Allergy Rates Grow, Connected Tech Creates Safety Net
- + A Realistic Look At IoT In Healthcare

64 In Focus

- + How Facial Recognition Technology Threatens Basic Privacy Rights
- + Making Sense Of Today's Security Camera Options
- + Leveraging The Biometrics Ecosystem To Improve Cybersecurity
- + Risk And Identity-defined Security Paramount As Attacks On Biometric Data Rise
- + Mobile Biometric Authentication: The Advantages And Disadvantages

Cover Story

24 | The Ins And Outs Of Event Security

Security Feature

37 | Mobile Apps: Insecure By Default

In Focus

76 | Mobile Biometric Authentication: The Advantages And Disadvantages

Incredible!

ASTM M50 ***Portable*** Barriers & Bollards



Available now, you can set up certified ASTM M50/P3 rated portable barriers and bollards on concrete, asphalt, compacted soils or vegetation in 15 minutes or less to provide M50 stopping power. Your people are now protected from damage by a 15,000 pound (6804 kg) medium-duty truck going 50 mph (80.4 kph). Quick deployment, multiple configurations and, best of all, unrivaled security at the highest level!



See our full line of certified crash tested portable and fixed line of vehicle access control products at www.deltascientific.com.



Link M50 rated TB150 bollards together to create immediate protection for spans of 20 feet (6 m) or greater. TB150's contain and stop 1.2 million foot pounds of medium-duty truck.



Visit www.deltascientific.com for details and specifications.
GSA 47QSWA18D003B ▲ 1-661-575-1100 ▲ info@deltascientific.com

CONTACT

PUBLISHER

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

EDITOR

CJ Chia
(sst@tradelinkmedia.com.sg)

GROUP MARKETING MANAGER

Eric Ooi
(eric.ooi@tradelinkmedia.com.sg)

MARKETING MANAGER

Felix Ooi
(felix.ooi@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)



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.



Images/Vectors Credit: Freepik.com / Unsplash.com / Pixabay.com

Designed by Fawzeeah Yamin

SECURITY SOLUTIONS TODAY

is published bi-monthly by
Trade Link Media Pte Ltd (Co. Reg. No.: 199204277K)
101 Lorong 23, Geylang,
#06-04, Prosper House, Singapore 388399
Tel: +65 6842 2580 Fax: +65 6842 2581
MCI (P) 084/05/2019 | ISSN 2345-7104 (Print)

Printed in Singapore by
Refine Printing Pte Ltd (L011/06/2019)

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 (Co. Reg. No: 199204277K)
101 Lorong 23, Geylang, #06-04, Prosper House,
Singapore 388399
Tel: +65 6842 2580 Fax: +65 6842 2581
Email (Mktg): info@tradelinkmedia.com.sg

China & Hong Kong

Iris Yuen
Room 1107G, Block A,
Galaxy Century Building
#3069 Cai Tian Road,
Futian District
Shenzhen
China
Tel: +86-138 0270 1367
sstchina86@gmail.com

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



MicroEngine®

Integrated Security Systems

The Trusted Brand in Security Solutions

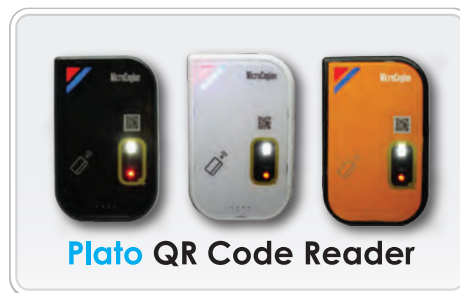
OnPremQR™

Mobile Identification System

NO CLOUD
NO SUBSCRIPTION



- Innovative QR Code based security system
- On Premise mode, no Cloud subscription
- Better option for Non Cloud-Ready Offices
- Clone detection with Dynamic QR Code
- Higher security using AES128 Encryption
- Works with our Integrated Security System



1300-88-3925 or enquiry@microengine.net

www.microengine.net



DESIGNED BY MALAYSIAN
MADE IN MALAYSIA



REG No. 749921389

COMING SOON

MAR
18 – 20
2020

SECON 2020

📍 Seoul, South Korea
☎ +82 2 6715 5400 🌐 www.seconexpo.com
✉ global@seconexpo.com

MAR
18 – 20
2020

ISC West 2020

📍 Las Vegas, USA
☎ 203 840 5602 🌐 www.iscwest.com
✉ www.iscwest.com/Forms/Customer-Service-Form/

APR
11 – 13
2020

IFSEC Bangladesh 2020

📍 Dhaka, Bangladesh
☎ - 🌐 www.ifsec.events/bangladesh/
✉ www.ifsec.events/bangladesh/about/event-contact

APR
22 – 24
2020

Secutech 2020

📍 Taipei, Taiwan
☎ +886 2 8729 1017, +886 2 8729 1099 🌐 www.secutech.tw.messefrankfurt.com/taipei/en.html
✉ kirstin.wu@newera.messefrankfurt.com, services@secutech.com

MAY
07 – 09
2020

Secutech India 2020

📍 Mumbai, India
☎ +91 22 4286 3869 🌐 www.secutechexpo.com
✉ info@secutechexpo.com, info@firesafetyexpo.in

MAY
19 – 21
2020

IFSEC International 2020

📍 19–21 May 2020
☎ London, UK 🌐 www.ifsec.events/international/
✉ ifseccustomerservice@ubm.com

JUN
23 – 25
2020

IFSEC Southeast Asia 2020

📍 Kuala Lumpur, Malaysia
☎ +60 3-0771 2688 🌐 www.ifsec.events/kl/
✉ ifseccustomerservice@ubm.com

JUL
22 – 24
2020

IFSEC Philippines 2020

📍 Manila, Philippines
☎ +63 2 551 7718 🌐 www.ifsec.events/philippines/
✉ www.ifsec.events/philippines/eform/submit/contact

AUG
20 – 22
2020

Secutech Vietnam 2020

📍 Ho Chi Minh City, Vietnam
☎ +886 2 8729 1099, +84 4 3936 5566 🌐 www.secutechvietnam.tw.messefrankfurt.com
✉ stvn@newera.messefrankfurt.com, project1@vietfair.vn

SEP
21 – 23
2020

Global Security Exchange 2020

📍 Atlanta, USA
☎ +1 888 887 8072, +1 972 349 7452 🌐 www.gsx.org
✉ asis@asisonline.org

A Smarter Way to Monitor Video

Avigilon Control Center 7 Software

Video Security, Transformed

Avigilon Control Center (ACC) 7 is the latest and most advanced version of ACCTM video management software. Designed to revolutionize how users interact with and gain situational awareness from their video security systems, ACC 7 software provides an easy-to-use, AI-enabled user interface helping ensure critical events do not go unnoticed.

Focus of Attention Interface

Introducing a new concept in live video monitoring, Focus of Attention, which leverages AI and video analytics technologies to determine what information is important and should be presented to security operators.

AI-Powered Analytics

Using our self-learning video analytics and Unusual Motion Detection technologies, ACC 7 software focuses the operator's attention on the most important events

Dark Mode

ACC 7 software introduces a new theme with colors specifically chosen to reduce eye strain in dark environments, such as video security control rooms.



avigilon.com/acc7 | asksales@avigilon.com

Dear readers,

Security arrangements for a large-scale event take a massive amount of effort. Maintaining and managing a large crowd includes a varied range of considerations from planning for medical emergencies to ensuring that no security risks get through. In today's landscape, keeping the crowd safe is of utmost priority. What are the security measures to put in place and what are the factors to consider when engaging a security company? In this issue, we look at the basics of planning security for large outdoor and indoor events. Learn more about the challenges of putting adequate security measures in place and discuss the tools that can be used to make your security arrangements more robust.

Home is where the heart is, which is why when there is a security breach in the house, it hurts even more. We place the spotlight on how advancements in technology have changed the security landscape in the residential and healthcare sectors. With increased connectivity comes renewed opportunities for malicious incursions into your network. We identify practices and policies which may be helpful in reducing these security risks.

Finally, we zoom in on the various types of surveillance cameras and biometrics authentications and discuss the considerations when setting up your security system so you can run your business with more peace of mind.

Happy reading!

CJ Chia

Editor



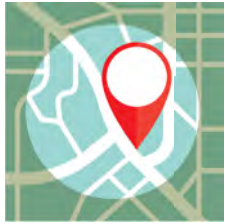
Superior Design Flexibility. More Installation Options.

ZETTLER makes it possible. Today's fire protection needs can be complex. That's why the PROFILE Flexible system from ZETTLER has been engineered to provide a powerful, versatile solution for virtually any fire protection application. With robust configuration software, a modular design and integration with standard BMS systems, it can meet even the most challenging requirements. Because protecting life matters. And safety should never be a compromise.



For more information about
ZETTLER and the PROFILE Flexible
product line, visit **zettlerfire.com**

SECURITY FLAWS FOUND IN 600,000 GPS CHILD TRACKERS



Researchers at Avast Threat Labs found vulnerabilities in 29 different devices commonly used to track the whereabouts of children, seniors,

and pets. These affected devices expose data that is sent to the cloud and enable hackers to lock on to the real-time GPS coordinates of the wearer, and make it possible for third parties to hack into devices and falsify data to give an inaccurate location reading.

Data being sent from the devices to the cloud was unencrypted, unauthenticated, and written in plaintext, making it an easy target for hackers. In addition, devices with built-in cameras and microphones were found to have flaws that make it possible for these functions to be used by hackers to spy or eavesdrop on the wearer.

The faulty devices were made by Chinese manufacturer Shenzhen i365 Tech and are resold under various brand names. Avast made their findings known to Shenzhen i365 but received no response.

Martin Hron, Senior Researcher at Avast, said: "We have done our due diligence in disclosing these vulnerabilities to the manufacturer, but since we have not heard back after the standard window of time, we are now issuing this Public Service Announcement to consumers and strongly advise you to discontinue use of these devices."

Avast advised people to steer clear of suspiciously cheap and knock-off smart devices, and noted that the use by children of even those tracking devices deemed safe from an information security perspective may affect their ability to learn how to be independent and may also give adults a false sense of safety.

WEAPONISED BLUEKEEP EXPLOIT RELEASED

Security researchers at Rapid7 and Metasploit released a new weaponised exploit for the BlueKeep vulnerability that exists in certain versions of the Windows operating system with the goal of helping users understand the types of attacks this vulnerability will allow if left unpatched, as well as letting security teams understand the steps to take to minimise risk and mitigate these issues.

Malicious activity connected to this vulnerability remains low at present, and no exploits have been detected aside from those released by security researchers. The exploit released by Metasploit had several limits put on it as safeguards, and applying the Microsoft patch for the vulnerability worked, making it highly recommended that users patch any remaining vulnerable machines as soon as possible.



GOOGLE BACKS OPEN SOURCE VULNERABILITIES HUNTER, SNYK

London and Boston-based start-up, Snyk Ltd., secured an additional \$70 million that will be used to continue expanding the business. The latest round was led by Accel Partners with participation from existing investors GV—Google's venture arm—and Boldstart Ventures.

Snyk got its start identifying and developing security solutions for developers who were working on open-source code, and has since expanded to building security solutions to help developers identify and fix vulnerabilities around containers, which has become an increasingly common software that is used to package and run code on different computing environments.

Open source is used in 95% of all enterprises, and Snyk estimates that up to 77% of open-source components that are liable to have vulnerabilities. Containers are a different issue. Although they are present in fewer than 30% of computing environments at present, their growth is on the rise; Gartner has forecasted that more than 75% of global organisations will run containerised applications by 2022. With 44% of Docker image scans showing known vulnerabilities, providing security solutions for this software is of great importance.

"Today, every business, from manufacturing to retail and finance, is becoming a software business," said Peter McKay, Snyk's new CEO. "There is an immediate and fast-growing need for software security solutions that scale at the same pace as software development. This investment helps us continue to bring Snyk's product-led and developer-focused solutions to more companies across the globe, helping them stay secure as they embrace digital innovation – without slowing down."

Part of the
ASEAN Super 8 Series



IFSEC

SOUTHEAST ASIA

SECURITY • FIRE • SAFETY

23 - 25 JUNE 2020

MALAYSIA INTERNATIONAL TRADE
AND EXHIBITION CENTRE (MITEC), KL



SECURITY IS CRITICAL IFSEC IS ESSENTIAL

Organised By



WWW.IFSECSEA.COM



@IFSECSEA #IFSECSEA



IFSEC Southeast Asia

UL AND VIAKOO COLLABORATE FOR PHYSICAL SECURITY SYSTEMS COMPLIANCE

Leading global safety science company UL announced a strategic collaboration with Viakoo, a leader in automated IoT service assurance solutions, in order to mitigate ongoing operational and cyber-hygiene issues which are commonly found in physical security systems.

The two companies will explore opportunities to help businesses maintain compliant physical security systems that remain resilient to cyber threats during their service lifespan.

The introduction of IP-based systems, the myriad cybersecurity threats, as well as increased reliance on video surveillance has contributed to the rapid transformation of the physical security industry. This in turn means that security systems that were correctly configured and functioned properly at the point of installation can quickly become non-functional. On top of this, these systems are often targeted by hackers and require ongoing assessment of vulnerabilities for effective cyber hygiene.

UL and Viakoo hope to develop solutions to tackle these challenges and strengthen security through their collaboration. "The relationship with Viakoo, a unique SaaS provider in the physical security space, coupled with UL's security domain experience and compliance expertise, has the prospect of helping end-users manage their growing connected technology infrastructure more efficiently, while reducing the overall risk of a critical system failure," said Neil Lakomiak, Director of Business Development and Innovation for UL.

INTELLIGENT SECURITY SYSTEMS TAKES FACIAL RECOGNITION BEYOND SURVEILLANCE

Intelligent Security Systems demonstrated the company's new powerful SecuOS™ FaceX analytics at GSX 2019. Transcending conventional facial recognition solutions which are solely for video surveillance, FaceX provides the high level of accuracy required to use facial recognition for access control ID authentication.

Ideal for mainstream single-factor and multi-mode access control applications, FaceX will provide system designers with a highly cost-efficient analytics solution for multiple use cases. SecuOS FaceX enables a host of facial recognition features and capabilities with the highest levels of accuracy and low false match rates. It can clarify a database search based on specific face features, from age, gender, and ethnicity, to hair colour, facial hair, and any accessories.

FaceX also resolves challenges for facial recognition related to viewing angles, facial expressions, and lighting conditions, and can compare captured images against databases or video streams, allowing the use of facial recognition to facilitate the search for individuals in real-time. SecuOS FaceX features also allow integration with multiple watchlists for security purposes and is able to provide the detailed reporting and metric needed to aggregate data for forensic investigations.



FIRST AUSTRALIAN IoT MASTERS COURSE LAUNCHED BY LA TROBE

La Trobe University revealed plans to launch a dedicated Master's degree specialising in the internet of things (IoT) in order to cater to growing demand in the sector. The city of Bendigo in Victoria, Australia will be used as a "living lab" to field test these new technologies.

Students of this program will explore a broad spectrum of IoT technology applications across different industries over the course of their studies. Alongside programming and systems design skills, courses will also cover security protocols and privacy risks – something critical for the networks

that can contain multiple devices that often have limited security capabilities and are constantly transmitting data. "The course is planned to be highly workplace-focused and hopes to teach students to be creative, clever, and adaptable to industry need," says Dr Simon Egerton, Head of La Trobe's Technology Innovation lab.

Besides partnerships with organisations in the city, La Trobe will also work with several multinational organisations to provide students with opportunities ranging from mentorship, travel scholarships, work placement, and field trips.

IFSEC

PHILIPPINES

SECURITY • FIRE • SAFETY
22 – 24 JULY 2020
SMX CONVENTION CENTER
PASAY CITY, METRO MANILA



THE LEADING **SECURITY, FIRE**
AND **SAFETY** EVENT IN PHILIPPINES

Organised By



WWW.IFSECPHILIPPINES.COM



@IFSECPH #IFSECPHILIPPINES



IFSECPHILIPPINES

JAGUAR LAND ROVER AND BLACKBERRY FOCUS ON SECURITY IN NEXT-GEN VEHICLES

Jaguar Land Rover and Blackberry have announced plans to deepen their partnership in the production of intelligent next-gen vehicles. A focus on security is central to the expanded collaboration of the two brands.

An increasing number of vehicles—cars in particular—have been manufactured to be fitted with advanced electronics, high-tech devices, and connectivity in recent years. This has enabled advances such as in-built GPS, internet access, vehicle health diagnostics, driver assistance, and even entertainment, but has simultaneously opened up new security risks. With cars essentially becoming mobile computers that are lacking in security sophistication, they are becoming more exposed and susceptible to being attacks by outside forces.

In 2015, researchers were able to remotely hack a Jeep Cherokee by targeting its entertainment system, and were able to gain access to the vehicle's dashboard functions, brakes, steering, and transmission. This investigation highlighted the potential for harm by malicious hackers, making this announcement from Jaguar Land Rover and Blackberry a welcome one.

"Jaguar Land Rover and BlackBerry share a common objective in bringing the most intelligent vehicles to reality," said Professor Sir Ralf D Speth KBE FREng, Jaguar Land Rover CEO. "I am delighted that our partnership with BlackBerry continues to go from strength-to-strength, a company whose technology innovations uniquely address the expanding safety needs of the automotive industry."

VERINT TRUSTED TO REDUCE FRAUD AND ENHANCE SECURITY

Verint Systems Inc. saw increased opportunities in the first half of this year from various enterprises utilising its intelligent solutions to support fraud reduction and enhance security operations.

As the financial industry evolves, threats faced by financial organisations continue to change. Amidst these growing threats, banks and credit unions continue to turn to Verint in order to identify the best ways of strengthening risk management using technology that simplifies, automates, and modernises their fraud and safety programs.

With more than 2,300 banking customers across the Americas, Verint's suite of advanced technology solutions has been proven to meet customer requirements for actionable intelligence, fraud detection, and compliance.

Verint also leverages on key relationships to continue providing the highest level of security. One such collaboration with Seagate helps to enhance customer privacy and secure critical data by creating a secure infrastructure that maximises the safety of video and security intelligence. The company also continues to further its commitment to the banking market with the addition of the Verint Video Investigator, a software platform that helps security personnel to mitigate risk by augmenting the ability to identify security threats in near real-time.

IBM INTRODUCES z15 MAINFRAME WITH SECURITY DATA PASSPORT

IBM has unveiled the latest incarnation of its mainframe, the z15 enterprise platform. Engineered to manage the privacy of customer data across hybrid multi-cloud environments, the server has been in development for four years and was created through collaboration with over 100 companies. It offers improvements to encryption, cloud native software development, and business continuity.

A new feature, known as Data Privacy Passports technology, will allow clients to control how data on the mainframe is stored and shared, giving them the ability to protect and provision data, as well as to revoke access at any time. This data security provision is not restricted to the z15 environment, having been built to work across an enterprise's hybrid multi-cloud environment.

The z15 can also encrypt data anywhere in order to help enterprises secure their data wherever it travels, IBM shared, claiming that these security enhancements allow organisations to establish and enforce enterprise-wide data privacy policies where users have access to different views of data based on what the user needs to know.

"Trusted Data Object technology can also be used to prevent collusion between data owners leading to the misuse of data, and can track the complete data transformation journey from point of origin to point of consumption, with a central point of auditing and compliance for all data access and aggregation," said IBM.

secutech

INDIA

Find effective pathways into Asia's fastest growing market

07 – 09 May 2020

Bombay Exhibition Centre
Goregaon (E) Mumbai India

www.secutechindia.co.in



messe frankfurt

INVIXIUM LAUNCHES ITS FULL RANGE OF BIOMETRICS SOLUTIONS IN SOUTH AFRICA

Invixium, a manufacturer of modern, IP-based biometric solutions marked its official launch into South Africa with an exclusive private event in Johannesburg.

Hosted in collaboration with their distribution partner Pyro-Tech, the event was held at the Sandton Sun Hotel, located in the heart of Johannesburg's economic hub for businesses and international travellers.

The audience comprised of top Access Control Panel Manufacturers, local system integrators and security consultants, were enlightened on the Invixium product offerings especially IXM TITAN, became acquainted with the portfolio during the live hands-on demos and appreciated the opportunity to ask their questions directly to the manufacturer.

The event was kicked off with brief introductions by Sandra Santos – Marketing Manager at Invixium, followed by Joe Ferreira – Managing Director of Pyro-Tech, who extended their gratitude to the audience on behalf of both companies for donating time out of their schedules to attend the event.

The highlight of the day was an impactful keynote presentation by Shiraz Kapadia – the CEO & President of Invixium, which covered the company's seven-year



history, philosophies, and offerings specific to the South African market. Shiraz's extensive 18+ years of experience in the biometric industry resonated with the audience as he confidently spoke about his "lessons learned" from his dramatic career shift from being the Chief Operating Officer at Bioscrypt to becoming the Founder of a startup company and also debunked many common myths about biometrics. Midway through the keynote and as an example of showing Invixium's differentiation, Shiraz revealed the superior performance of SENSE 2 equipped with Lumidigm's multispectral imaging sensor by successfully authenticating with a wet finger live on stage.

THETARAY CONTINUES GLOBAL EXPANSION WITH MEXICO OFFICE LAUNCH

ThetaRay, the leading provider of AI-based big data analytics, announced the opening of its Latin America headquarters in Mexico City, Mexico. The new location will provide local support for ThetaRay's Latin American customers, assisting them in the detection of financial cybercrime schemes. It is ThetaRay's fifth office worldwide, joining those in Israel, the United States, the UK, and Singapore.

"Our Mexico office grants us the opportunity to become a leading provider in the important Latin America region, and to better assist our customers in the fight against global financial cybercrime," said Mark Gazit, CEO of ThetaRay. "ThetaRay is

experiencing considerable growth and success in 2019, and we are enthusiastic about continuing our global expansion."

The banking environment in Latin America is in dire need of ThetaRay's solution to find "unknown unknown" financial crimes that cannot be detected by legacy systems. In Mexico alone, more than fifty top financial institutions are suffering today because they do not have a best-in-class solution to fight terrorist financing, professional money laundering, narco trafficking and other malicious acts. The office will be overseen by LatAm Managing Director Felipe Mora Cervera, who has 12 years of

experience providing technology and information services to Latin American financial institutions. He has also collaborated with multiple government agencies, providing expert insight on fighting crimes such as money laundering, fraud, corruption, slavery and human trafficking.

"Our team in Mexico has over 40 years of combined experience fighting financial cybercrime, and is well positioned to provide excellent local support to our growing Latin American customer base," said Benjamin Wyrick, SVP sales for ThetaRay. "We are also eager to work and partner with additional financial institutions in the region."

SILVERSHIELD™ SHOWCASES VISITOR AND INFORMATION MANAGEMENT SOLUTIONS

SilverShield™ showcased their award-winning visitor and information management system at GSX 2019. The easy-to-use, cloud-based SAAS approach to security has several different modules that provide a complete safety solution for different requirements.

The SilverShield Visitor Management System enables both staffed and unstaffed visitor screening at different types of facilities, from schools, medical facilities, or even businesses that need to screen visitors and maintain records. The multi-platform solution allows users to quickly screen a visitor's credentials against watchlists and other offender databases in near-real-time, enabling users to decide if the visitor should be welcomed or denied entry. Should a threat be identified, the system also allows the user to immediately send silent alerts to designated stakeholders via a two-way communication mode. In the case of organisations with unstaffed entrances, the SilverShield Kiosk System allows visitors to register themselves either manually or by scanning a valid ID, and will increase security and safety at unmanned entry points.

Other systems on display included the Incident Management module which could alert local police and initiate a virtual lockdown in cases of an emergency situation; the SilverShield's HR & Safety Resource Center, which organisations can use to store their security plans in a secure Learning Management System (LMS) and share it with staff and stakeholders as necessary; and the Event Management System which screens guests against watchlists and offender databases, ensuring that no unwanted guests are invited to the events inadvertently.

SUPERMICRO SERVERS AT RISK FROM USBANYWHERE VULNERABILITIES

A set of vulnerabilities has been discovered in Supermicro servers, which allows remote attack on systems as long as threat actors have physical access to the USB ports. Researchers at Eclypsium discovered the flaws in the baseboard management controllers (BMCs) of Supermicro servers, and dubbed the issues "USBAnywhere". Since BMCs are intended to allow administrators to perform out-of-band management of a server, these authentication issues put servers at risk. The problem stems from the way that BMCs on Supermicro X9, X10, and X11 platforms implement virtual media; when accessed remotely, the virtual media service allows plaintext authentication, sends most traffic unencrypted, and uses a weak encryption algorithm which is susceptible to an authentication bypass for the rest.

Using these issues, an attacker is able to easily gain access to a server by capturing a legitimate user's authentication packet, using default credentials, and even without any credentials in some cases. To understand these vulnerabilities and develop fixes, Supermicro engaged with Eclypsium and released firmware updates for affected systems. In addition to making these firmware updates, Supermicro has also advised users to disable virtual media by blocking TCP port 623.

ASSA ABLOY ANNOUNCES INTEGRATION OF WIRELESS LOCK TECHNOLOGY



ASSA ABLOY Opening Solutions announced the integration of their wireless lock technology with the Pinnacle Advanced access control software and 1700 Intelligent Controller from Sielox LLC. This integration adds superior access control management and control capabilities that address the most demanding needs today, whilst also being a scalable solution for the future. Sielox's 1700 Intelligent Controller will allow a fully distributed 32-bit access control panel that is able to provide facility protection, even in the scenario that communications have been interrupted. The unit has been proven in the field and can connect directly to a network, resulting in cost-savings for the user.

Sielox's award-winning Emergency Notification and Response Solution also improves situational awareness, which saves time and has the potential to save lives in emergency situations.

"Aperio is a superior wireless lock that not only provides a high level of security but helps dramatically reduce installation costs," said Karen Evans, President & CEO of Sielox LLC. "By integrating the Aperio lock with our Pinnacle and CLASS software and controller, we are giving customers the ability to implement wireless access in conjunction with existing hardwired access to provide a layered security solution."

PAYMENTWORLD PARTNERS XCALIBER SOLUTIONS FOR A ROBUST FRAUD AND CHARGEBACK MANAGEMENT PLATFORM

PaymentWorld, a payments technology company, announced a partnership with Xcaliber Solutions Inc. that will bring together a robust fraud and chargeback software platform. With this addition, PaymentWorld encompasses a tool that comes with a full fraud platform built-in from Xcaliber Solutions, Verifi, Ethoca, and 3-D Secure.

Card-not-present (CNP) fraud losses are expected to reach \$130 billion between 2018 and 2023. As a result, it is more crucial than ever for online merchants to implement a robust fraud solution to protect their sales. But managing multiple integrations and systems can be time-consuming and complex.

PaymentWorld's platform includes a suite of world-class fraud prevention and chargeback management tools built-in so merchants can accept more orders, from more customers, and in more places than ever before. The PaymentWorld platform includes:

- Xcaliber Solutions – By combining technology and unmatched expertise, Xcaliber fully manages chargebacks to protect businesses against invalid disputes and friendly fraud, with the goal of recovering



lost revenue, reducing risk and protecting their bottom line.

- Ethoca & Verifi through Xcaliber – Verifi CDRN and Ethoca Alerts can stop chargebacks before they happen and can prevent up to 40% of fraud and non-fraud related chargebacks so businesses keep more sales.
- 3-D Secure – PaymentWorld supports 3-D Secure, with all the major card programs, to authenticate Card-Not-Present transactions behind the scenes for a friction-free consumer experience. This lets businesses implement an additional layer of protection and comply with any regional or card type requirements or mandates.

- Tokenisation – Replacing real card data with secure token.
- Fraud Tools – Velocity Filters, Address Verification, Card Verification, Geo IP Tracking, Negative Database, and so much more.

“Our goal is to help businesses accept credit card payments without a constant worry of fraud. We strive for a seamless solution that allows merchants to fraud-proof their payments with a single integration to our processing software,” said Roman Balanko, CEO, PaymentWorld.

Sabina Keil, COO of Xcaliber Solutions Inc, added: “We are very proud to have been chosen as PaymentWorld’s technology experts in chargeback management. An increase in chargebacks, declines and refunds is not sustainable long term and effective dispute management is vital for today’s merchants.”

PaymentWorld helps merchants protect their businesses by giving them the power to accept orders from multiple sales channels through a single solution. PW’s platform increases payment conversions through enhanced fraud and risk management.

GK8 UNVEILS TECHNOLOGY FOR SENDING TRANSACTIONS WITHOUT INTERNET CONNECTION

Israeli start-up GK8, which provides secure end-to-end management of digital assets, has completed the development of a patented technology for sending transactions to the blockchain without any direct or indirect internet connection. GK8 is now emerging out of stealth mode and announcing that it has completed a seed funding round of \$4 million, led by Check Point co-founder Marius Nacht and Israel Discount Capital, Israel Discount Bank Investments Arm, with the participation of investors such

as the blockchain VC firm EdenBlock, iAngels, IDEAL-HLS, StratX and Israel Innovation Authority. GK8 is currently targeting financial institutions, custodians, exchanges and hedge funds which hold cryptocurrencies. GK8’s custodian technology is already operational and helps to securely manage digital assets for clients such as eToro, a global multi-asset trading and investment platform. GK8’s customers manage a total of more than \$1 billion in digital assets.

To be continued on page 19

Current custodian solutions used by financial institutions and state-owned enterprises do not meet institutional scale security standards. In addition to existing security protocols, digital assets based on blockchain technology need a higher security standard since signed transactions are irreversible.

Unfortunately, the current blockchain wallet solutions, categorised into "cold wallets" and "hot wallets", are subject to major cybersecurity vulnerabilities. Cryptocurrency thefts, scams, and fraud worldwide led to the stealing of approximately \$4.26 billion in the first six months of 2019 alone.

To meet this challenge, GK8 experts have developed proprietary cryptographic techniques that enable real-time blockchain transactions of digital assets without any need for an internet connection. These techniques provide a secure environment to sign blockchain transactions and execute automatic reconciliation confidently. The company's

techniques, protected by five registered patents, can bypass core assumptions related to cryptocurrency transfers and eliminate attack vectors to any asset transfer.

These capabilities allowed GK8 to develop the world's first and only secured cold wallet with hot wallet functionalities. As a result, digital asset transfers secured by GK8 become inaccessible to criminal hackers or sponsored cyber-attacks. Based on these capabilities, GK8 developed a fully operational end-to-end encrypted system for managing and safeguarding digital assets beyond the reach of hackers.

Lior Lamesh, co-founder and CEO of GK8, noted: "Shahar Shamaï, GK8's co-founder and CTO, and I, found security vulnerabilities in one of the most secured cold wallets in the market. After we saw how easy it was, we understood that hackers will invest millions to steal billions, and we decided to develop a secured end-to-end institutional tool for managing digital assets."

QOGNIFY ANNOUNCES CYBER SECURITY RELEASE OF CAYUGA VIDEO MANAGEMENT SYSTEM

Trusted advisor and technology solution provider for physical security and enterprise incident management Qognify announced that the latest release of its video management system (VMS) Cayuga R14, places a major focus on cyber security.

With the rise of IP solutions for video surveillance systems in recent years, dealing with cybersecurity issues to safeguard video installations has become of utmost importance. One of the best ways to reduce network vulnerabilities associated with video surveillance systems is to make sure that the communication between the different components of the video solution is securely encrypted. A comprehensive role-based access management must also be in place in order to elevate the level of protection, while meeting the compliance requirements of mission-critical environments.

Cayuga R14 is focusing on just that: the security architecture of the VMS has been revamped to make sure that internal communication is even



safer than before. State-of-the-art encryption is used for the export of videos, so that they can only be accessed by authorised people.

Fundamental Active Directory (AD) optimisations make sure that the login procedure for Cayuga and the administration of AD roles are now fully aligned with industry standards. As Single Sign On is now fully supported, there is no need to explicitly sign in to the Cayuga application – once the Windows login was successful.

Aside from all the security improvements, Cayuga now offers

the option to start the standard client in Viewer mode. This way the user benefits from most of the standard features in the client – even without a connection to the Cayuga server. The new offline Client is also available in a light-weight portable version to be distributed with exported video files.

Furthermore, Cayuga now supports more than 5,000 different devices from more than 80 different hardware manufacturers. New camera functions have also been introduced into its smart drivers, giving customers even more choice when selecting the right hardware for a video security application.

LEADING BANK IN INDONESIA ESTABLISHES HIGH VISIBILITY NETWORK

NTT Ltd. announced that it was chosen by a leading Asian bank in Indonesia to implement SD-WAN to optimise existing network bandwidth utilisation, improve critical application performance, and boost network visibility across more than 120 branches.

NTT was appointed to redesign and optimise the bank's connectivity, which was identified as one of the key areas on the bank's journey to transform itself into a premier bank through innovation and growth.

The proposed solution includes a SD-WAN solution that uses a fully redundant Multiprotocol Label Switching (MPLS) link with an active-active connection that ensures faster response time.

By allowing granular visibility of network traffic across all branches, anomalies in user behaviour traffic can be closely monitored and attended to immediately.

Dimension Data Indonesia's Country General Manager, Hendra Lesmana said, "In today's digital era, banks must be agile, innovative, and customer-centric. To do this, they should leverage high performance solutions that allow them to quickly adapt to changing customer requests and market demands. We are thrilled to be working with one of the region's leading banks that is committed to helping small and medium enterprises and retail partners thrive. We believe that our close collaboration will support the bank by accelerating their services locally and across the region. It will also address their dynamic bandwidth requirements and greater network visibility, ultimately playing a key role in their digital future success."

ONESECURE ASIA PARTNERS WITH ACCEDIAN TO ENHANCE VISIBILITY-AS-A-SERVICE SUITE

Singapore-based Managed Security Service Provider (MSSP) Onesecure Asia announced its partnership with Accedian in order to enhance their 'Visibility-as-a-Service' offerings.

This partnership provides enterprises with complete visibility into their IT infrastructure performance across different platforms, enhancing performance, and strengthening their resilience against cyber threats.

The Visibility-as-a-Service solution offers threat monitoring services on top of end-to-end network and application performance visibility, and empowers Small and Medium Enterprises (SMEs) and start-ups to gain insight into their operations and the user experience of their end users without having to invest in an internal security operations centre. With an increasing number

of businesses going digital, the risk of exposure to potential online threat has increased, meaning that there is a strong need for SMEs to have a robust cybersecurity system that can detect threats early and diagnose issues quickly. Nearly 56% of SMEs in Singapore experienced a cyber incident in 2018, highlighting the vast visibility gap between cyber threat and their readiness in handling them.

"As enterprises go digital, having a holistic view of their IT infrastructure will become a critical component of a strong and resilient digital presence. By partnering with Accedian, we are now able to offer companies the ability to control the cybersecurity and performance of Physical and Virtual infrastructure through complete infrastructure visibility," said Edmund How, Managing Director of Onesecure Asia.

CERULEAN GLOBAL SERVICES LEVERAGES COMCAST BUSINESS SOLUTIONS

Cerulean Global Services (Cerulean) selected Comcast Business to install 100Gbps circuits between the company's San Jose and Rancho Cordova, Calif. Data centres to enable these data centres to become secure destinations for expanding Asian enterprises into U.S. markets.

With Cerulean as a reputable and reliable carrier, the data centres and their client enterprises will have the opportunity to tap on an efficient data circuit and storage exchange. Leveraging on Comcast Business's 100Gbps circuit capacity,

clients will be able to bypass the multiple stops that are typical for sharing large amounts of data, instead connecting point-to-point and helping international providers

and customers to send and receive large amounts of data to and from the U.S. market.

Comcast Business provides a variety of market leading global enterprise solutions that help businesses

grow, innovate, and transform industries. With Comcast Business' help, Cerulean can provide Asian enterprises access to more than 35 million customers in its data centres.



SURGE IN PIRACY OF CONTENT AMONGST ONLINE CONSUMERS

A study of the content behaviour of Filipino consumers revealed that 34% of consumers use a TV box which can be used to stream pirated television and video content. These TV boxes often come pre-loaded with illegal applications allowing 'plug-and-play' access to pirated content. This latest study shows a substantial increase compared to a similar study undertaken previously and highlights the detrimental effects of streaming piracy on legitimate subscription video services.

"The proliferation of Illicit Streaming Devices (ISDs) in the market as an access of pirated content affects the livelihood of people in the local creative and film industries. There is a need to continue educating the public that online piracy is unsafe and can put data privacy and devices at risk. We encourage everyone to watch content



using legitimate sources only," Ernest Cu, Globe President and CEO, said.

The problem is not restricted to Philippines, with piracy being a problem across the region. A study commissioned by the Asia Video Industry Association's Coalition Against Piracy (CAP) revealed that 23% of Malaysian online consumers use ISDs to stream pirated content, and 50% of all online consumers have used piracy streaming websites to access premium content.

NATIONAL UNIVERSITY OF SINGAPORE (NUS) EMPOWERS STUDENT ETHICAL HACKERS

Students from the National University of Singapore (NUS) benefited from HackerOne's training and expertise during the university's bug bounty challenge with the platform. As part of NUS' forward-thinking approach to secure its infrastructure and bridge the cybersecurity skills gap, the university launched the three-week hacking challenge in August 2019.

More than 200 students took part, hunting for security vulnerabilities in NUS' digital infrastructure with bounties ranging from US\$100 to US\$1,500 depending on the severity of the discovered vulnerabilities.

"Rather than just focusing on the technical aspects of the programme, we wanted our students, even those who had never tried hacking before,

to learn something new out of this. So, prior to the contest, we collaborated with HackerOne to provide training for the students in the form of webinars, online eLearning, and sample hacking exercises," said Professor Tommy Hor, Chief Information Technology Officer for NUS.

At the conclusion of the challenge, 13 valid vulnerabilities had been reported by students, with US\$4,550 awarded in total. Participating students were also eligible to earn extra academic credits on relevant course modules upon the completion of the training sessions.

NUS plans to make the hacking challenge an annual event, and expects to expand the scope of applications to be tested in 2020.

GEOSPARK ANALYTICS FORMS STRATEGIC PARTNERSHIP WITH INTERNATIONAL SOS

Disruptive technology experts Geospark Analytics will work closely with International SOS, the world's leading medical and security risk services company. Through this partnership, the organisations will utilise Geospark Analytics artificial intelligence capabilities to monitor and forecast emerging events and trends.

Geospark Analytics industry leading Hyperion Artificial Intelligence (AI) platform will become an integral part of International SOS analytics, exclusive in the travel risk industry, and will be an important complement to unique source information and expert analysis. These will in turn be used to advice on employee risk levels and mitigation recommendations for managers, as well as direct to companies' global workforces.

The Geospark Analytics cloud compute architecture calculates millions of permutations of activity and stability relevant to the security environment, across different countries, regions, and even at the city level.

"As a pure play AI-driven platform that is vertically integrated into the security and threat space, we are excited to bring the power of Hyperion to International SOS and their Security Intelligence and Operations Centers across the globe," said Omar Balkissoon, Founder and CEO of Geospark Analytics. "The combination of International SOS' medical and security risk expertise and Hyperion's industry leading AI-forecasting is a natural partnership showing applied AI at work pushing International SOS's mission forward. We are proud to be part of their team ensuring safety and security in more than 90 countries."

McAfee WARNS SINGAPOREANS TO CLEAN UP THEIR DIGITAL ACT

Revealing findings from their research into Singaporeans' attitudes to social media hygiene, McAfee shared that four in five Singaporeans own up to being embarrassed by their social media. Almost one in five admit that they've either never, or can't remember the last time they checked their timelines, something concerning especially since lax privacy settings mean posts can be seen by a prospective employer. It is also important to take a closer look at privacy settings in order to prevent the wrong people from stumbling across damaging and personal content. Despite how important this is, 16.8% of respondents had no idea how to change their privacy settings on social media, and a whopping 43.2% have not taken steps to protect their private information despite having the know-how.



"It's always a good practice to watch what we post, but sometimes we do not follow good social media hygiene. Many Singaporeans have abandoned social media accounts that are not deleted, leaving behind personal information and old photos that could be seen by potential peers and employers, or worse, cybercriminals looking to harvest data for personal gain," commented Shashwat Khandelwal, Head of Southeast Asia Consumer Business, McAfee.

SINGAPORE AIRLINES REIMAGINES EMPLOYEE DIGITAL EXPERIENCE WITH VMWARE

Singapore Airlines (SIA) selected VMware, Inc.'s Workspace ONE solution to provide a richer employee digital experience across multiple apps and device. With the focus on augmenting SIA's mobile-friendly Bring Your Own Device (BYOD) strategy, VMware Workspace ONE platform aims to streamline the delivery of mobile applications across both employee-owned and company-issued devices.

The platform will facilitate seamless access to SaaS productivity applications as well as SIA's mobile and intranet web applications on BYOD mobile devices. Consumer-focused ease of access and usability coupled with the delivery of enterprise-level security for corporate data has helped to drive higher employee engagement across the organisation. Using Workspace ONE's App Catalog, SIA has successfully deployed 35 mobile applications developed by its in-house technology development and innovation team, reflecting SIA's commitment to provide a mobile-friendly experience for an increasingly mobile-first workforce.

VMware's Workspace ONE compliance engine enables all applications to meet compliance and compatibility requirements, allowing applications to remain fully functional and up-to-date with the latest security patches and providing the best employee experience without compromising on the airline industry's strict security standards.

ST ENGINEERING LAUNCHES INAUGURAL CYBERSECURITY OPERATION CENTRE AS-A-PLATFORM (SOCaaP)

ST Engineering's Electronics sector has launched the first-of-its-kind Cybersecurity Operation Centre As-A-Platform (SOCaaP), which will deliver customised security operations centre (SOC) solutions that will result in greater operational efficiency and significant cost savings for customer's digital assets.

The SOCaaP provides a complete suite of capabilities to protect, detect, respond to, and recover from cyberattacks, and includes cutting-edge technologies such as a new age Security Information and Event

Management (SIEM) and Advanced Analytics Engine. These capabilities will provide an organisation's network with automated, real-time analysis of security alerts with a higher degree of accuracy, compared to existing solutions.

The Electronics sector entered into a collaboration with Myanmar partner, Alliance Urban Transports (AUT) to provide cybersecurity services and training for Myanmar's government, financial services, and insurance sectors. ST Engineering and AUT will jointly operate an SOC in Yangon.

Through SOCaaP, the setup of this SOC will be shortened to just under four months, from the usual over 12-month lead time required for such implementation. The partners will also operate a cybersecurity training centre in Yangon to help strengthen Myanmar's national cybersecurity resilience and boost its cyberthreat detection and response capabilities. To date, ST Engineering has delivered more than 15 SOC's for government agencies and commercial enterprises internationally, helping them maintain a secure environment while ensuring continuity of business operations.

NETFOUNDRY™ SPINS OFF INTO A NEW INDEPENDENT SUBSIDIARY OF TATA COMMUNICATIONS



Tata Communications, a leading global digital infrastructure provider, announces that NetFoundry™, a software and business developed as part of Tata Communications' Shape the Future innovation and entrepreneurship programme, has become an independent subsidiary within the Tata Communications Group. NetFoundry passed the \$1 million USD annual recurring revenue (ARR) milestone in less than two years of selling its services, growing ARR by over 50% on a quarter-over-quarter basis for the past three quarters. Through this spin-off, Tata Communications aims to help the North Carolina-based company to accelerate its growth further.

"By spinning off NetFoundry, we want to help this innovative, ambitious start-up boost its speed of execution and capture a larger share of a nascent market," says Tri Pham, Chief Strategy Officer, Tata Communications. "This is an exciting milestone for not just NetFoundry but also for Tata Communications' Shape the Future, setting a great precedent for scaling other similar breakthrough ventures from this programme."

The NetFoundry™ platform eliminates the complexity and cost of traditional business networking. It spurs innovation by enabling customers to programmatically embed private networking into their applications and solutions. The result is that application providers, cloud and system integrators, managed service providers and leading-edge businesses can deliver applications across any set of edges and clouds, with zero trust security and optimised performance, and without relying on configuration, private circuits or custom hardware. Customers control their networks via NetFoundry's web console, APIs and SDKs. They can access NetFoundry's global Software Defined Network (SDN) from any Internet connection, while NetFoundry manages all the underlying infrastructure in a Network-as-a-Service (NaaS) model. NetFoundry's software is available in leading cloud and edge marketplaces, such as AWS, Azure, CoreSite, Digital Ocean and IBM Cloud.

The SaaS start-up is one of the first ideas conceptualised, incubated, and funded as a breakthrough idea under Tata Communications' Shape the Future. This programme offers a platform for Tata Communications' employees to innovate and create new businesses. These businesses are supported by Tata Communications but operate and grow as independent start-ups, using agile processes and systems.

nCIPHER NSHIELD HSM ACHIEVES BUREAU OF INDIAN STANDARDS (BIS) CERTIFICATION

nCipher Security, an Entrust Datacard company and provider of trust, integrity, and control for business-critical information and applications announced that its nShield Connect XV hardware security module (HSM) is now certified by the Bureau of Indian Standards (BIS). Organisations in India now have access to a BIS-approved, high-assurance security foundation to protect their sensitive data, network communications, and enterprise infrastructure from cyberattacks.

nShield HSMs are hardened, tamper-resistant appliances that perform functions including encryption, digital signing, and cryptographic key generation and protection. With their comprehensive capabilities, nShield HSMs support an extensive range of applications, including certificate authorities and code signing.

As the national standards body of India, the BIS sets parameters for ensuring the quality, safety, and reliability of products entering the Indian market, and is mandatory for many IT products, including HSMs. By earning BIS certification for nShield Connect XC HSMs, nCipher reaffirms nCipher's position as an HSM market leader, committed to helping customers meet compliance needs around the world. Over 1,000 organisations rely on nCipher HSMs, including 5 of the top 10 Fortune 100 companies.

"nCipher has long championed best practices and industry standards. Achieving BIS certification demonstrates our commitment to the Indian market and to the highest security standards and compliance requirements," said Philip Schreiber, regional director, Middle East, Africa and South Asia at nCipher Security. "We are pleased that the BIS has certified nCipher's ability to meet its high cybersecurity standards."

THE INS AND OUTS OF EVENT SECURITY

Security at mass events can be a tricky field to navigate. Be it indoor or outdoor, your plans need to account for the scale of the event. Stay prepared for the worst-case scenarios to keep attendees and the public safe.

By CJ Chia

SECUR



One of the biggest challenges when organising an event is ensuring that it is safe for everyone involved. Large scale events require temporary arrangements and provisions need to be customised to handle big crowds, especially during the peak periods. Your security team might not be as familiar with the venue as compared to one which is stationed at a permanent location, and with the increase in risk of terrorism at event venues, it's important to guard—not just the boundaries of your event venue—but also the surroundings to ensure threats are not able to get close enough to do any harm.

Contracting a security company that understands the nuances of event security is one of the most important to-dos of a large event. Event security guards must be able to maintain and manage a large crowd. This is an already difficult task that gets worse when alcohol is served on the premises. An experienced security team must be able to handle the situation carefully and quickly so as to not disrupt the event.

First and foremost, when liaising with an event security service company, you must ensure that the company operates in agreement with all policies in the state where the event is held. The security company must have a personal patrol operator license and accountability insurance. The company also needs to hire personnel who hold valid security personnel licenses and have passed thorough background checks. After confirming that your security company operates in accordance with state regulations, we recommend that you review the types of events and properties that have provided security in the past. Since many regional contract security companies cover a variety of events, it is important to find a company that specialises in events of the required crowd size.

In addition, there is a bonus if hired guards are first aid and CPR certified. Large music festival-style events often forget to account for crowd dehydration, heat stroke, and other health risks. Deploy security officers who can address basic medical needs so that attendees can get immediate attention.

Event venues are often large spaces with different alcoves throughout, making them ideal places for potential security threats. A pre-event venue inspection checklist is important for security staff to familiarise themselves with the space which they will be working in. During the pre-event inspection, the event planner and security team must determine all security checkpoints, officer positions, points of interest, and other special requirements for specific venues and events.

After the event is over, it is important for planners and security teams to report and review how security operations were performed. This exercise will ensure that all parties are aware of where they succeeded, as well as highlight any areas for improvement. If an incident occurred that was not handled properly, this review is an opportunity to figure out what went wrong and ensure that it doesn't happen again. The review process also gives supervisors the opportunity to applaud more advanced security personnel and identify those who need additional training. In the words of John F Kennedy, "There are risks and costs to a program of action — but they are far less than the long-range cost of comfortable inaction."

Security Challenges Of A Large-scale Event

It's time to update the practice on risk assessment plans. Broadly speaking, there are three main parts to the risk assessment plan, ensuring that the people involved can hold the event as safely as possible.

- **Danger identification:** Recognise the danger associated with the event. To identify these risks, consider the different people involved and their role in setting up, running, and participating in the event. You need to recognise not only human-related hazards, but also technical, natural, and environmental hazards.



- **Risk assessment:** Use the risk assessment matrix to estimate the potential impact of a hazard and ascertain the level of risk. Once you do this, you can prioritise the most pressing risks.
- **Risk management:** Start with a high level of risk and develop a rational solution with the help of the event team. These include hazard elimination, substitution, engineering, management, and the use of appropriate safety equipment. Above all, you need to look for a logical and practical solution.

When planning the event, you will probably have considered how many people can be accommodated in the venue. However, from a security standpoint, it is recommended that you choose an event perimeter that extends beyond the minimum requirements for your needs. This is because security problems tend to occur in densely populated areas. For example, panic and uncertainty can lead to crowd disasters like stampedes. By expanding the event area and having additional event security, you can reduce some of that risk.

Management of event data also comes with its own set of challenges. Gone are the days when Excel spreadsheets or notebooks were acceptable for event data recording and management. As security needs grow, there is a need to look at technical solutions designed to manage your data more efficiently. For example, event websites should

adopt the Secure Sockets Layer (SSL), which encrypts the link between the web server and the browser. This ensures that the data sent between the two remains encrypted.

Safety and security also extend beyond what is happening at the event location. It is important to manage data related to an event and its participants. When collecting data about customers, you must comply with data protection laws. This applies to all types of information, from event attendee names and addresses, to data collected through more sophisticated techniques such as attendance tracking.

A mobile event app is a great tool for collecting event data, but before you start using it, you need to make sure that your app developer has the right security measures in place. In particular, you need to make sure that only authorised personnel have access to the data. Establish an approval process to grant access to these personnel, while ensuring that everyone else is unable to access this information through any loopholes.

Different Types Of Security Arrangements

Sporting events, festivals, concerts, conferences, fund raisers, political campaigns, and other events, tend to attract crowds and thus may become the targets for crimes such as theft, robbery, assault, and terrorism. These events become bigger targets as crowds assemble and grow. They

may also become opportunities for special interest groups to publicly demonstrate. Poor event planning, management, crowd control, security, and ineffective emergency response increase the likelihood of injuries, property damage, and even catastrophic attacks.

There are different aspects to consider when planning for public events. Security should be focused on the following elements:

- **Guest list monitoring**

Ensure that only authorised personnel can gain access to various rooms. Special security is needed to support this. Ensure that they are aware of or are able to identify people who are working at the event. To allow them to perform this function,

you must make sure to provide them with the necessary tools and documentation.

- **Pay attention to parking security, cars, and guest valuables**

Security officers need to keep vigilant for the security of vehicles and any stored valuables in the parking lots, and know how to stop criminals who want to make a fuss or cause trouble.

- **Call EMS service in case of a medical situation**

As a precaution for any medical situation that might occur, have security officer(s) who can contact the relevant EMS service on-site to assist, as well as to manage the crowd, and prevent possible interference in the event of a major medical incident.

- **Provide deterrence that is visible to intruders**

It's important to have security personnel in highly visible positions to deter any unsavoury characters who might be entertaining the possibility of compromising the safety of your

event. Security personnel might need to wear uniforms and carry arms depending on your risk assessment of the event.

Security Differences Between Outdoor And Indoor Events

One of the first things to learn in a security career is that the two types of venues have different security requirements. Every event venue has a special set of considerations that must be identified and carefully handled by the team. Narrow corridors can raise safety concerns in the event of a fire or other emergencies. Conversely, in large, open arena settings, it can be difficult to identify fraudsters. It is the responsibility of the security officer to evaluate each venue and determine the best procedure and protocol for the event at hand. You can start by dividing the event into one exact dichotomy: indoor events and outdoor events.

- **Indoor venue**

The enclosed and sealed nature of indoor events are both a blessing and a curse for security teams. On one hand,





it is generally much easier to secure and control the exit point for indoor events. On the other hand, a large crowd in small venues can quickly become dangerous to themselves if not properly policed. The security team must be careful that the guest list does not exceed fire safety regulations. In an emergency, the auxiliary exits must be carefully managed so that guests can leave in a safe and orderly manner.

CCTV systems installed in prominent positions can serve as a powerful deterrent against potential criminals in indoor events. In many cases, security teams can maintain order and prevent criminal activity simply by maintaining a visible presence at indoor events. In general, people commit crimes only if they are confident that they can escape from the crime scene. The intimidating presence of a competent security force will deter most people from causing trouble. For indoor events, it is easier to maintain the “sky eyes” watching your every move, which in itself, is a powerful deterrent.

When operating in an indoor venue, the importance of fire safety cannot be emphasised strongly enough. In an enclosed area, fire can spread quickly and do harm in a short period of time,

and it is important to consider an advanced fire detection system for maximum safety.

One example of well-executed security for indoor events is the integrated technology solutions implemented by Siemens to secure the Salzburg Festival in Austria. Considered the world’s finest drama and classical music festival, over 200 events take place at 14 different performance venues each year. To ensure maximum safety and security, Siemens installed over 1,800 fire detectors to monitor the different areas throughout the festival halls. Smoke extraction systems were also deployed to over high-level protection of the audience and stage areas, and clear instructions are given via a voice alarm system in cases of an emergency.

- **Outdoor venue**

The two main challenges typically associated with outdoor events are perimeter security and crowd management. To maintain perimeter security, small patrols with two-way radios should be spaced out throughout the event venue. This allows patrols to quickly identify and

respond to security threats that could potentially compromise the safety of guests. This system can also promote effective crowd control measures. In an emergency, patrols should be no further than 30 feet of each other. This allows individual patrols to adjust to the situation quickly and converge as needed in response to dangerous situations.

Access control is also key in an outdoor venue, where there is a lack of checkpoints that guests will need to go through, and that security can be concentrated at. To circumvent this, it becomes necessary to create access points through the use of barricades and the like. In these cases, automating access rights through high-tech solutions will make your task easier, with the security team better able to concentrate on looking out for other risks.

For an example of the usefulness of access control, one needs to look no further than the solution deployed at the famous 24 hours of Le Mans Circuit by the Automobile Club de l’Ouest (ACO). With many facilities in close proximity of the track, there are hundreds of different access points which require a variety of permissions, ranging from permissions for ACO employees to the circuit’s customers, such as Porsche, and even fans. To implement a suitable solution, ACO turned towards LOCKEN’s Cyberlock solution, which uses a rechargeable digital smart key and innovative software to ensure perfect traceability for all stakeholders.

For outdoor events, it may be easier to coordinate with a local law enforcement agency. By leveraging an existing local police presence, private units may be relieved of the stress of protecting the surroundings of the event venue.

High Tech Tools For Large Scale Events

Let us take a closer look at the technical tools to improve event

security. There are different types of events that require security, from private parties to large rock festivals, and the tools used to heighten security are offered in a variety of shapes and sizes, supporting a wide range of applications.

Certainly, technical tools are only as good as operators, and tools are often a means of identifying suspicious items and people. Ideally, such identification is done before the event and away from the potential target to create time and space between the potential threat and the victim.

Event security technical tools can be divided into three main types, depending on their role in the protection procedure.

- **Threat deterrence**

Physical security techniques limit unauthorised access to the event itself and to restricted areas within the event boundaries. It also manages the crowd and helps event guests move in controlled lines rather than surge towards the entrance en masse.

Turnstiles are particularly useful with a large number of access points when there is a need to check a large number of people before they are allowed access to restricted areas. This tool is even more effective when used in combination with a scanner that reads credentials to speed up the authentication process.

Name badges and ID cards are an important part of security for events such as exhibitions and conferences. At the simple end of the range, a security staff uses these badges to identify guests and staff who have access to specific areas by checking the barcode, using a colour code or scanner.

Another type of physical security technology useful for even security is CCTV surveillance. Cameras are a simple but useful way to discover and monitor new threats, and keep an eye on the movement of individuals,

groups, and crowds at large events. Agents can also find threats in the crowd and be aware if there is a group of people being made to stand down in an area, which will help to speed up their response times in the event of a threat.

Similarly, a **thermal camera** like Flir reveals important information about changes in crowd density. This allows event security staff to find “hot” areas which might endanger event guests.

Fence or barrier **contact pressure sensors** detect and record the pressure the crowd exerts on the barrier. This allows event security staff to have real-time information about barrier hotspots and take precautions.

- **Threat identification**

A **security wand** or **handheld metal detector** helps agents find weapons or other metal objects.

Walk-through metal detectors, also called magnetometers, are suitable for large crowds where many people need access in a short time. Both CEIA and Garret offer great options and the portable solution is relatively easy to carry.

Using an **X-ray scanner**, agents can inspect weapons, explosives, bottles, and other items (cargo if necessary).

Sniffer dogs: Some may argue against calling a four-legged colleague a “technical tool”, but it should be included in this list anyway. K-9 EDD (aka explosive detection dog) has proven effective in detecting explosives (and even cannabis), and event security managers can use them for both pre-event sweeps and spot checks during the event depending on the need.

- **Accident management**

The most important tool for managing event incidents are **emergency medical kits**. Well-trained event security staff must be able to provide emergency care when needed.

A **GPS tracker** is also useful to identify the geographical location of security staff, healthcare professionals or assets which are needed to help manage incidents. With trackers, administrators can locate people and things and direct them to other locations as needed. Geo-fencing can also be set up so that an alarm goes off when a person or asset enters or exits a designated area.

The **operations centre** gathers all the relevant information and communications in one place. Technologies used here include monitors, software, and communication tools.



IoT And Home Automation: What Does The Future Hold?

Once a dream, home automation is slowly but steadily becoming a part of daily lives around the world. In fact, it is believed that the global market for smart home automation will reach \$40 billion by 2020.

By Rushabh Patel, Founder and CEO of Siddhi InfoSoft

These days, there is a vast range of devices powered by IoT. These include thermostats, refrigerators, security systems, and even dryers and kettles. With the passage of time, more devices are sure to be added and with smarter features.

Smart Homes And Internet of Things

Before proceeding any further, let's take a closer look at IoT. 'Internet of Things' is an umbrella term used for all technologies that enable the connection of a device to the Internet.

Such systems depend on the collection of data. The data is then used for monitoring, controlling and transferring information to other devices via the internet. This allows specific actions to be automatically activated whenever certain situations arise. In a simple example, consider a smart kettle. The kettle can be programmed to automatically turn off once it reaches a specific temperature. It might also send a notification to the user on the same.

Now apply the same concept to the entire home and all the devices present. That is a smart home powered by IoT. Instead of manually going up to the device and taking action, those actions can be taken at the press of a button. These

days, most smart home automation devices allow you to control them via an app or even via voice commands. Now imagine if you did not even need to undertake such actions. In other words, the smart home will know when to take certain actions and automatically take them. This is where the future of home automation and IoT lies.

Here are some possible scenarios that we may see in future.



Lighting

These days, smart lighting is all the rage. They can be scheduled to turn on/off and change their intensity. However, in future, it is possible for this to be taken a step further. With IoT enabled across the home, the lights can respond to other actions you take.

For example, the lights can respond to your home cinema. They can turn off or dim whenever you start watching a movie. Going further, they may even react to the type of movie. For example, they can turn off completely if the lights sense that you are watching a horror movie, giving you the proper atmosphere.

Doors

In the future, doors can become smarter as well. Imagine them opening only when you enter or close. This may be



made possible via a smart device or facial recognition. This can be taken to the next step by getting the rest of the house take actions in tandem with your entry.

For example, the lights can turn on as soon you as enter through the door. Alternatively, if you are leaving, they can turn off.

Windows

Windows can become smarter as well. Imagine them automatically open the shutters when the sun rises and close at sunset. You may even be able to program them to close automatically when it rains. Consider the previous example of a home movie. Your curtains can lower whenever you are watching a movie.

Thermostat

These days, you can control your home thermostat remotely via apps. In the future, you may not even need to do that. The thermostat will be able to recognise if you are nearing your home. It will then check the room and external temperature and set the right one for you. It may even recognise when you are taking certain actions and adjust accordingly such as when you are showering or exercising.

Gardens

Even your gardens can become smarter in the future with IoT. You will be able to place IoT sensors in the garden. If

these sensors detect dryness in the soil, they can trigger the irrigation system. Robotic lawnmowers can be automatically deployed if the grass exceeds a certain height.

Home Routines

It is already possible for much of the home to be connected with smart devices. There are smart sockets that automatically turn on/off devices. Smart alarms can play music when you wake up or even tell you the news. Voice assistants can even run entire routines where the lights, home appliances, thermostat, alarms and other devices are controlled.

Going forward, this will be extended throughout the home. Consider the morning routine. The shutters will open right before you wake up to help you get rid of that grogginess. Even before you wake up, the coffee maker will start getting your morning cup ready. The bathroom will get the water heated for your shower. Your stereo will start playing some morning tunes as you have your morning cup. Your TV will also turn on and show you your preferred news channel. Of course, the thermostat will adjust to a comfortable temperature.

Of course, all of these are not going to happen overnight. There are a few barriers to widespread adoption of IoT-enabled smart homes, the primary of which is cost. Privacy is another major concern. Then there are the current technological limitations that create difficulties in a seamless connection between multiple IoT devices.

Securing Consumer IoT Devices: Why A Global Standard Is Needed

For consumers, the growth of the Internet of Things (IoT) means more and more objects in their home are now linked to the internet, and are potentially at risk of cyberattacks, or of revealing personal data in privacy breaches.

By Alex Leadbeater, Chairman of ETSI Cyber Security Technical Committee (TC Cyber)

Over the last few years, there have been increasing numbers of reports of consumer IoT problems with cyberattacks. For example, security researchers recently discovered that ZipaMicro, a smart home hub, used the same private key in each hub, hardcoded into the devices. Combined with scrambled passwords they found on the internet, researchers were able to open locks controlled by the hub.

Devices at risk include connected toys, which may well contain cameras and microphones that can be remotely accessed. As well as attacks over the internet, some toys now use Bluetooth, which is a potential weakness. Smart speakers, such as Amazon's Echo, are also vulnerable to hackers listening in on private conversations,

These kinds of problems are usually fixed quickly by device vendors once they have been alerted in new products, but that may be too late and there is an inconsistent approach to fixing or recalling those already in the market. Governments are attempting to bring in legislation to mandate higher standards – for example, the UK is consulting on new laws, which may include compulsory labelling of products and minimum standards. The US is not far behind, with California already banning generic default passwords. Then in terms of data protection, there are laws such as the EU's GDPR



that apply to any stored personal information. But this can make life difficult for product vendors – how can they ensure that they cost-effectively meet different sets of requirements in different countries, in a fast-changing market where regulations are still being defined?

Standard Provides Security Recommendations

To address this problem, ETSI recently announced ETSI TS 103 645, the first global standard for consumer IoT security. The new standard aims to establish a benchmark for how companies should secure any consumer products that will be connected to the internet, and to promote best practice.

At the same time, it has been written with a focus on outcomes rather than specific methodologies, which means there is sufficient flexibility to enable companies to innovate and find the best solution for their particular products. The standard aims to address the needs of a wide range of connected devices, including toys, wearable fitness trackers, smart home assistants, smart TVs, door locks, and home automation systems.

Let's look at the advice in ETSI's new standard, and how it will make connected consumer devices more secure.

Device Requirements

First off, the standard says that all device passwords must be unique – overcoming the problem today where many products are sold with a default username and password, which users often don't change. It also says it should be impossible to reset the password back to a default. It is surprising that many products on the market do not meet this or other more basic requirements in the new standard already.

Personal data protection is an important part of the standard, and it requires all sensitive information to be stored securely – both on devices themselves, and in any related services, such as in the cloud. Devices must not have credentials hard-coded, as these are relatively easy to discover.

The products need to make it easy for consumers to delete their personal data when they want to, with clear instructions provided. Similarly, installation and use of IoT devices needs to be simple and well-documented. Data must also be protected and encrypted when it's being communicated. Devices must provide suitable protection against attacks on encryption.

All connected devices need to follow good security engineering practice, such as closing unused software and network ports to minimise the risk of attack. Any data inputted should be validated, to prevent exploits such as the use of out of range values. Devices must also be able to verify their software using some kind of hardware-based



secure boot mechanism, and to handle any power or network outages successfully.

As well as requirements for the devices themselves, the ETSI standard has specific demands for product vendors. These include seeking out and acting on vulnerabilities promptly. Device software must also be able to be updated easily and securely.

Building Consumer Confidence

Consumers are justifiably concerned about IoT security. The new standard is an invaluable way for vendors to rebuild trust with their customers. By following its guidance, manufacturers can ensure their products meet appropriate levels of security and privacy. This means that customers are protected, and companies can avoid costly breaches, and the impact of negative publicity.

More importantly, the ETSI standard is a step change for consumers, giving them confidence that their safety, privacy, and security will not be put at risk by using connected devices.

Security Challenges For The Future Of IoT

Internet of Things (IoT) is one of the hottest technologies in the era of digital transformation, connecting everything to the Internet. It is the core technology behind smart homes, self-driving cars, smart utility meters, and smart cities. But there are nine main security challenges for the future of the internet of things (IoT).

By Vaibhav Shah, CEO of Techuz

The number of IoT devices is rapidly increasing over the last few years. According to an analyst firm Gartner, there will be more than 26 billion connected devices around the world by 2020, up from just 6 billion in 2016.

While IoT devices bring effective communication between devices, automate things, save time and cost, and have numerous benefits, there is one thing still concerning the

users—IOT security. There have been specific incidents which have made the IoT devices challenging to trust.

Several smart TVs and cash machines have been hacked, which is negatively impacting the trust of not only consumers but also enterprises. Having said that, let's have a deep dive into the most critical security challenges for the future of the Internet of Things (IoT).

1. Outdated Hardware And Software

Since the IoT devices are being used increasingly, the manufacturers of these devices are focusing on building new ones and not paying enough attention to security. A majority of these devices don't get enough updates,



whereas some of them never get a single one. What this means is that these products are secure at the time of purchase but become vulnerable to attacks when the hackers find some bugs or security issues.

When these issues are not fixed by releasing regular updates for hardware and software, the devices remain vulnerable to attacks. For every little thing connected to the Internet, the regular updates are a must-have. Not having updates can lead to data breach of not only customers but also of the companies that manufacture them.

2. Use Of Weak And Default Credentials

Many IoT companies are selling devices and providing consumers default credentials with them – like an admin username. Hackers need just the username and password to attack the device. When they know the username, they carry out brute-force attacks to infect the devices.

The Mirai botnet attack is an example that was carried out because the devices were using default credentials. Consumers should be changing the default credentials as soon as they get the device, but most of the manufacturers don't say anything in the instruction guides about making that change. Not making an update in the instruction guides leaves all of the devices open to attack.

3. Malware And Ransomware

The rapid rise in the development of IoT products will make cyberattack permutations unpredictable. Cybercriminals have become advanced today – and they lock out the consumers from using their own device.

For example, an IoT-enabled camera that captures confidential information from home or the work office – and the system is hacked. The attackers will encrypt the webcam system and not allow consumers to access any information. Since the system contains personal data, they can ask consumers to pay a hefty amount to recover their data. When this occurs, it's called ransomware.

4. Predicting And Preventing Attacks

Cybercriminals are proactively finding out new techniques for security threats. In such a scenario, there is a need for not only finding the vulnerabilities and fixing them as they

occur but also learning to predict and prevent new threat. The challenge of security seems to be a long-term challenge for the security of connected devices. Modern cloud services make use of threat intelligence for predicting security issues. Other such techniques include AI-powered monitoring and analytics tools. However, it is complex to adapt these techniques in IoT because the connected devices need processing of data instantly.

5. Difficulty In Locating Affected Device

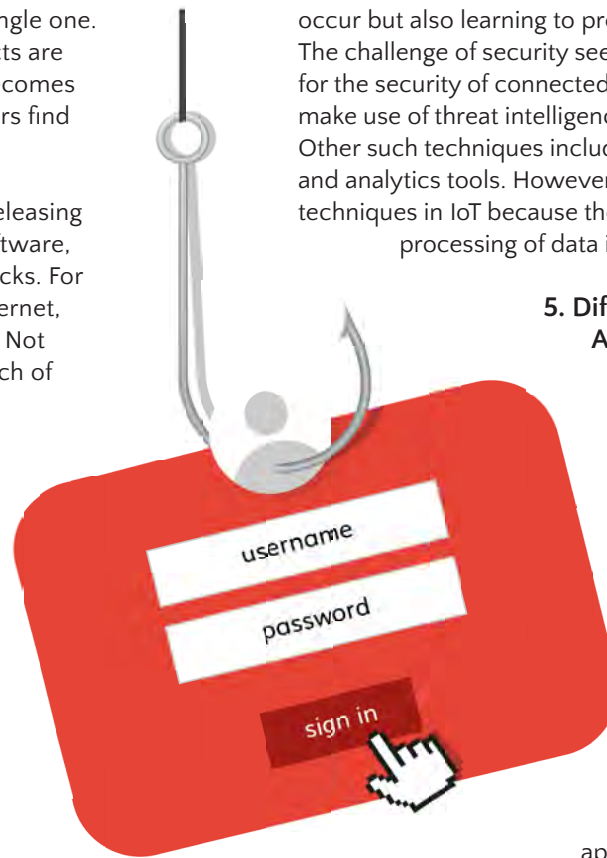
Although it is not really possible to guarantee 100% security from security threats and breaches, the thing with IoT devices is that most of the users don't get to know if their device is hacked.

When there is a large scale of IoT devices, it becomes difficult to monitor all of them even for the service providers. It is because an IoT device needs apps, services, and protocols for communication. Since the number of devices is increasing significantly, the number of things to be managed is increasing even more.

Hence, many devices keep on operating without the users knowing that they have been hacked.

6. Data Protection And Security Challenges

In this interconnected world, the protection of data has become really difficult because it gets transferred between multiple devices within a few seconds. One moment, it is



stored in mobile, the next minute it is on the web, and then the cloud.

All this data is transferred or transmitted over the internet, which can lead to data leak. Not all the devices through which data is being transmitted or received are secure. Once the data gets leaked, hackers can sell it to other companies that violate the rights for data privacy and security.

Furthermore, even if the data doesn't get leaked from the consumer side, the service providers might not be compliant with regulations and laws. This can also lead to security incidents.

7. Use Of Autonomous Systems For Data Management

From data collection and networking point-of-view, the amount of data generated from connected devices will be too high to handle.

It will undoubtedly need the use of AI tools and automation. IoT admins and network experts will have to set new rules so that traffic patterns can be detected easily.

However, use of such tools will be a little risky because even a slightest of mistakes while configuring can cause an outage.



This is critical for large enterprises in healthcare, financial services, power, and transportation industries.

8. Home Security

Today, more and more homes and offices are getting smart with IoT connectivity. The big builders and developers are powering the apartments and the entire building with IoT devices. While home automation is a good thing, but not everyone is aware of the best practices that should be taken care of for IoT security.

Even if the IP addresses get exposed, this can lead to exposure of residential address and other contact details of the consumer. Attackers or interested parties can use this information for evil purposes. This leaves smart homes at potential risk.

9. Security Of Autonomous Vehicles

Just like homes, the self-driving vehicles or the ones that make use of IoT services, are also at risk. Smart vehicles can be hijacked by skilled hackers from remote locations. Once they get access, they can control the car, which can be very risky for passengers.

In Summary

Undoubtedly, IoT is a technology that should be called a boon. But since it connects all the things to the Internet, the things become vulnerable to some sort of security threats. Big companies and cybersecurity researchers are giving their best to make things perfect for the consumers, but there is still a lot to be done.



Mobile Apps: Insecure By Default

Mobile applications have unlocked a world at your fingertips but can also open a door for hackers looking to steal your personal information.

By Taylor Armerding, Security Expert at Synopsys Software Integrity Group

They are the best of apps. They are the worst of apps. At the same time.

Mobile applications have unlocked a world of almost magical convenience, communication, and creativity. With a few swipes or taps on your smartphone you can buy food, clothes or just about any other product, pay your bills, chat with your friends, watch your far-away nieces, nephews or grandkids grow, monitor your exercise goals, take video

and stills of your vacation, listen to your favourite podcasts or music and more. Ever so much more. You can even turn your smartphone into a flashlight or use it to tune your guitar. But then, mobile applications can also unlock your personal, medical and financial information to hackers. They can make it possible for criminals to drain your bank account, eliminate your privacy – pretty much ruin your life.

And that is all, or at least mostly, because the large majority of mobile application developers spend their time and money hoping to dazzle their customers with bells and whistles, not on protecting those customers. Their apps are feature rich and security poor.

So it is no surprise that yet another research report—this one from Positive Technologies—finds that they are a high-risk convenience.



The company studied 17 mobile apps and reported finding high-risk vulnerabilities in 43% of the Android apps and 38% of those for iOS.

As noted, this simply confirms what others have found. The Naked Security blog provided a partial list: "The news won't come as much of a shock to anyone who has read GPEN's 2014 study of app privacy failings; IOActive's 2013 study of banking app security, nor its follow up in 2015 nor its investigation of stock trading app security in 2017; nor Arxan's 2019 look at banking and finance app security."

The Report

Among the highlights—or lowlights—of the report:

- Insecure data storage is the most common problem, found in 76% of mobile apps, putting passwords, financial information, personal data, and correspondence at risk.
- 89% of vulnerabilities can be exploited using malware, which means hackers rarely need physical access to a smartphone to steal data.
- Most vulnerabilities are the result of weaknesses in security mechanisms, not just in the apps themselves but on the server, which is hosted by the developer and with which apps communicate. The researchers found such weaknesses in 74% of apps for iOS and 57% of Android apps, with 42% for server-side components.

And they noted, "Because such vulnerabilities creep in during the design stage, fixing them requires significant changes to code."

User carelessness can play a role as well. "Many cyberattacks rely on user inattention. Escalated privileges or side-loaded software can pave the way for a damaging attack," the report said.

Why Are Mobile Apps So Insecure?

All of which raises the usual, fundamental questions: Why is insecurity so rampant on apps that are carried on billions of mobile devices? And what can be done about it?

The answer to "why" is pretty much what it has been since applications became mainstream. Amit Sethi, senior principal consultant at Synopsys, notes that it is not just mobile apps that are riddled with vulnerabilities. "Most developers tend to focus on features, performance, usability, etc. because the requirements they are implementing tend to focus on those areas," he said. "Also, there is always a rush to get features implemented, and security is often neglected."

Phillip Dunkelberger, president and CEO of Nok Nok Labs

and a founding member of the FIDO (Fast Identity Online) Alliance, an organisation that seeks to replace passwords with other, multiple forms of authentication, put the question to members of his team. Among the responses: "App developers often focus on the features that are most 'relevant' from a business perspective. Competing against convenience, usability and more, security sometimes does not make the top of the list."

Or as Grant Douglas, associate principal consultant at Synopsys, put it, the existing incentives don't promote mobile application security. "Developers are not only not incentivised, but security isn't always something a developer is exposed to through study and training," he said.

Perverse Incentives

In short, even with breaches and privacy violations in the headlines daily, the market incentives are still to get a feature-rich app into production as quickly as possible. If mobile app security is a casualty of that, so be it – the priority is not letting a competitor get to the market first. The irony, as any good security experts will tell you, is that good security doesn't slow development down. It can actually speed it up.

Yes, it can look both time-consuming and expensive. Sethi notes that creating secure apps "requires performing different activities during different phases of the software development life cycle (SDLC), such as threat modelling, static analysis, dynamic analysis, etc."

To that, developers should add software composition analysis (SCA), which helps developers find and fix any vulnerabilities or license problems with open source software components.

Make It Easy For Build-in Mobile App Security

But there are tools to help with those tasks. "Security teams can provide developers with easy ways to do the right thing," Sethi said. "They can create libraries that make it easy for developers to implement functionality in secure ways."

And Douglas said developers are increasingly open to "building security in" to mobile apps during the SDLC, especially when it can be a more seamless part of the process. At least some of them also see the long-term benefit – it takes less time and money to fix vulnerabilities early and throughout development than to try to patch dozens to hundreds of bugs that penetration testers find just before an app is due to go into production.

"Many frameworks exist for mobile platforms that cover security concerns and allow developers to abstract themselves from some of the more challenging decision/implementation woes," he said.

Thomas Richards, principal consultant at Synopsys, agreed. "Designing security in is the best approach and is also the cheapest," he said. "Setting security requirements early on and performing threat modelling can eliminate many security issues before code is written."

Not Getting The Message

But, as yet another study finds, the message isn't getting through enough of the time. Billions

of people are walking around with a virtual data bomb—dozens of bombs—in their pocket. According to App Annie, the average smartphone user has 60–90 apps installed on his or her phone, uses around 30 of them each month and launches nine per day.

What will it take to change the current reality? Users could demand better mobile app security. "If they are willing to pay more for solutions with robust security than for ones without, organisations will take action," said Dunkelberger's team member.

But the reality is, they haven't yet and likely won't. As Bruce Schneier, blogger, author and CTO at IBM Resilient Systems said years ago while lobbying for more aggressive government regulation of Internet of Things (IoT) security, consumers "don't care because they don't know enough to care."

Other Solutions For Mobile App Security

So, other options? Dunkelberger's colleague offered two: "Entities with regulatory power, such as App Store providers like Apple or Google, or government regulatory entities, must require a minimum level of security. And a practical approach would be to change the platform APIs [application programming interfaces] that are secure by default."

Enable Developers To Build Security Into Mobile Apps

Douglas agrees that while users bear some responsibility for their own security while using apps on their mobile devices, such as using secure passwords and not installing apps from untrustworthy sources, "the onus does fall mostly on the developers. They control how and where data gets stored, how long it gets stored, how secure that data is. The developers control how authentication works, how



frequently the user has to re-prove their credentials, etc."

Zach Lanier, principal research consultant at Atredis Partners, said beyond making security part of design, development and testing, developers should educate themselves "on the benefits and shortcomings of their stacks—everything from the languages and frameworks they use to the security features of the platform(s) on which they build—and ensuring they take advantage of those features where possible."

Do Authentication Better

Most experts agree that for both developers and users, the only way to make mobile app security mainstream is to make it easy. Convenience will trump security every time.

Lanier said part of that is transparency—that developers should notify users "about what changes or updates they make, especially as it relates to addressing any security issues that have been identified."

For Dunkelberger, one practical way to do that is to make authentication more robust with that method.

"With FIDO, the API is crafted carefully to be secure by default, and the authenticator is implemented by the platform, supporting various methods to verify the user—not only PIN, but also biometrics," he said. "Additionally, the authenticator can ask the user to provide the required verification data—taking the mobile app out of that equation."

Better authentication is indeed one significant way to improve mobile app security. But as Richards notes, it is still the responsibility of developers "to develop their application securely and consider security risks early and often while developing and supporting the application." And we're still waiting for that to happen.

Giving Consumers Responsibility In IoT Security Regulation

The UK government's plans to create regulation for IoT devices follows a broad global trend to try and lock down the burgeoning but insecure world of the IoT.

By Mike Nelson, VP of IoT Security, DigiCert

For too long now, Internet of Things (IoT) devices have been thrown to market replete with vulnerabilities that threaten strange new types of catastrophe for users. From attacks that leverage the very functionality of an IoT device—such as a hackable car or a doll that can be turned into a remote surveillance device—to events like the Mirai attacks which threatened internet infrastructure on a large scale. It's for those reasons that the UK government has stepped up.

The regulations aim to build on 2018's Code of Practice—Secure by Design—which offered a number of guidelines to IoT device manufacturers, as well as consumers, about how to securely build and use IoT devices. They include suggestions for securely storing credentials and other security data, minimising exposed attack surfaces, ensuring the integrity and continuous updating of the software on IoT devices as well as ensuring secure communication to and from the devices.

The code of practice added that it was being rolled out with the hope that people would comply, and if they didn't, the government would start to make those guidelines mandatory. That's finally happened and regulators will now make at least three of those guidelines compulsory.

The Three Guidelines

Firstly, IoT passwords have to be unique and not resettable to a factory default, thereby allowing an attacker to merely look that password up.

Secondly, manufacturers must have a publicly advertised contact for vulnerability disclosures, allowing bugs to be reported and fixed in good time.



Thirdly, manufacturers must clearly state the minimum length of time that the device will receive security updates, so that consumers can plan for offboarding or make other security decisions on that basis.

The devices that do comply will be able to proudly wear a stamp which signifies a government endorsement of this particular product's security. It might seem like a simple move, but it's one that profoundly changes the relationship between IoT security and the consumer.

IoT Security Left To Manufacturers

While IoT security has heretofore been left up to manufacturers and then perhaps enterprise security teams to fix after the fact, Secure by Design's

certification scheme finally puts those security decisions in the hands of the consumer. Now, they can make those decisions before they introduce weakly protected, vulnerable devices into an otherwise secure network.

Now that consumers can take security into account when purchasing IoT devices, it can become a competitive differentiator. Manufacturers until now have created insecure devices largely because it was cheaper for them to do so. There was no market demand to make secure devices and not much that would make it profitable for them to do so.

Labelling devices and introducing security as a competitive differentiator for consumers will force manufacturers to think about how they can lose

less and make more by thinking about security from the design stage onwards. Once consumers care, manufacturers are going to start caring too.

Calculation Made Too Late

It's a simple calculation which has been made far too late. For too long, the buck has been effectively left to manufacturers to secure their IoT products, with neither a carrot nor a stick to drive them forward. It won't solve all of the security problems but it's a commendable answer to a problem that has dogged this field for a long time. Governments around the world are starting to make sticks, but the clever thing about Secure by Design and its certification scheme is that it comes with a carrot too.



Game-changers For Smart Residences

A closer look at the trends and technologies transforming the smart home, and how integrators can take advantage.

**By Avi Rosenthal, Managing Partner
for Bluesalve Partners LLC**

It seems like the residential security industry is in a constant state of change. We took a look into the crystal ball to identify nine trends in this market and how they can affect your business in the months and years to come.

The Growing Value Of Data

The digital age has turned everything into data. Beyond facts and numbers, digital code contains images, events, choices, trends and more information that can be acted on, monetised and more. The Internet of Things connects all the electronic items that can measure, collect and forward this data for analysis. The ability to analyse and manipulate unstructured data has produced technologies such as voice recognition, face and event recognition, remote control and action, and AI to name just a few.

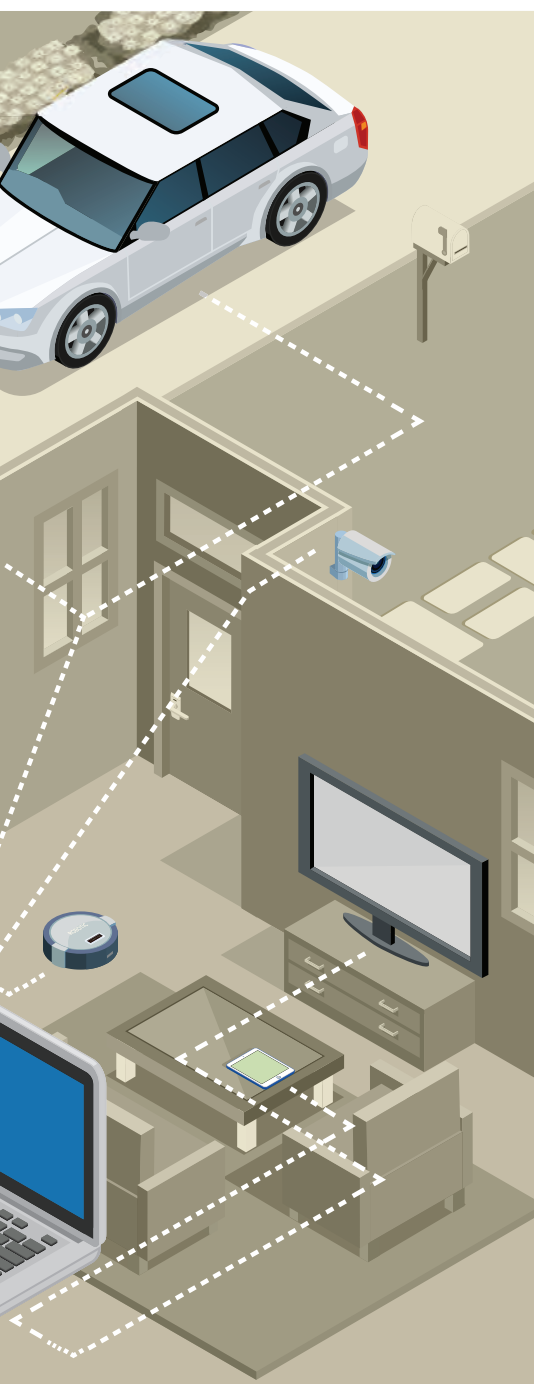
These capabilities have spawned new services in access control, maintenance, energy management, security and more to come that we simply have not yet thought of. Security companies can profit from this data by adopting and providing these new services to enhance scope; however, giant tech firms like Google and Amazon can do so as well. While Google or Amazon may use this data primarily to help sell through advertising, or by personalisation of offers to the consumer, it is important to understand that they consider this data so valuable that they subsidise other services as a path to get more of it – security being one of them.

Consumers are becoming aware of this; in fact, many are “creeped out” by online tracking, while others are worried about identity theft or the misuse of private information. This creates challenges surrounding both cybersecurity and privacy. These are the issues of our day, and service and



equipment providers must understand their place in securing systems as well as protecting customer privacy. While this can be viewed as a threat, there is good reason to believe that emphasising and selling these services creates a profitable and differentiated path.

Consider the overall value of the data your services generate, and then think about how you can use this to extend



services and build revenue. Decide whether partnering with or competing against the large data wranglers is the way to go. Figure out what your customer wants, and you too can get a slice of the value.

DIY

Is do-it-yourself a friend or foe to the security pro? The answer is both. On the positive side, the growing DIY security market has increased awareness of the security and home control product categories available. As more consumers become interested in these technologies, many will shop around for solutions – including in the professional market.

DIY will also impact professional business models—for example, the market is already seeing an increase in non-contract monitoring. Another possible business model change is to distribution channels—with consumers buying products online or from a retailer but preferring a professional to do the installation. This is called the DIFM (Do-It-For-Me) option.

The biggest potential negative to pros is that pure DIY solutions may become “good enough” to completely cannibalise the professional security market in the same way digital photography did to Kodak and film-based cameras.

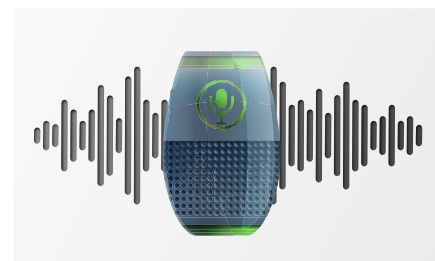
Evolving Sensors

There are many types of new multi-sensors available today—with more coming on the horizon—that give residential integrators new ways to understand their customers' environment and to provide better data collection, giving customers more choices about how to use that data.

These new sensors—from water sensors that do not need a plumber to install, to occupancy sensors that track people without motion sensors or cameras (they use RF waves)—will open new opportunities for the integrator, including aging-in-place

(more on that later), insurance cost reduction and increased RMR options. Additionally, increased battery life is reducing truck rolls, and radios are getting better, which further reduces customer support issues.

Voice Control



When it comes to integrating products into homes, it is easy (and normal) for a business to stick to a model that has worked in the past; however, controlling security by voice is something that often seems counterintuitive to residential security professionals. That said, security controlled by voice fits an emerging lifestyle where seamless integration in phones, automobiles and homes is not a feature – it is becoming an expectation.

Whatever platform(s) you choose, you will need to offer voice, not just as an option, but as a key ingredient in your systems. Google Home, as an example, offers the opportunity to create custom commands and responses, so you can involve your customers in the process of creating a system customised to their needs and syntax. Other providers have partnered with Amazon Alexa to expand the control of the security ecosystem.

Video's Explosion

As more security systems move to digital, interactive solutions, customers have garnered a better understanding of the value proposition of regular alerts and notifications from activity within and around their home. One of the biggest drivers of this increased popularity and resulting retention is video cameras, which have quickly

become a key requirement in residential security systems. Being able to see when the kids are coming home from school while at work, that a pet is safe and comfortable, or that activity on a front porch is a raccoon instead of an intruder, provides peace of mind that is obviously valuable to consumers. Technology and innovation in video also adds value for consumers, with features such as facial recognition, package detection, creating hot zones for the triggering of specific notifications or recording, and 24/7 streaming and recording. Practically all of these are baseline requirements for camera performance in today's marketplace.

Beyond the sheer comfort and enjoyment that customers get from a more interactive solution, many municipalities are considering video verification as a requirement before police dispatch in the event of an alarm.

Partnering With The Insurance Industry

For years, homeowners have received a discount on their home insurance premium with verified home security systems. Today, insurance companies now want access to the data that the security system is collecting so they can make better risk mitigation decisions about a home and its contents, and they are willing to pay for that data – typically in the form of a discount or lowered deductible (the better and more consistent the data, the better the discount).

The opportunity for integrators is providing systems that best fit the bill for the insurance company to give that discount and charge for the connectivity between the customer and the insurance company. Through partnerships, the integrator has the ability to tap into that stream of revenue and reap the benefits of the increased collection of data and the reduction of risk for the insurance company.

Increased Vehicle/Home Connectivity

Today's newest vehicles include an app that enables users to interact with the vehicle to lock/unlock, open the trunk and remote start. In the home, consumers can use a smartphone to interact with devices including lighting, HVAC and door locks. The next step will see these ecosystems working together. For example, based on the location of a vehicle (leaving or coming home), the home will automatically be put in home or away mode,

with the alarm armed/disarmed, lights on/off, doors locked/unlocked, etc.

This blending of the home and vehicle ecosystems presents both challenges and opportunities to integrators. The challenge is that today, unlike 30 years ago, vehicle manufacturers are leading the way on these connected technologies, which has significantly impacted the aftermarket electronics market. The opportunity is that vehicle manufacturers will be unlikely to offer support to the home ecosystem. A residential integrator is perfectly situated to combine both ecosystems for a customer.

Biophilia

A growing trend is the idea of "Living Well"—which comes down to clean indoor air quality, circadian lighting and mental health—and the security integrator has many technology options to offer here. More efficient HVAC and control systems monitor and maintain fresh air in spaces, venting hydrocarbons when necessary and closing vents when the outside air is worse than the indoor air. Lighting controls adjust the colour (or temperature) of the lights as well as the brightness during the day to relieve the occupants and produce better sleep patterns. All the while, these technologies are collecting data about the living spaces, the temperature, relative humidity, the amount of light coming in from windows, and the quality of the air.

Aging In Place

One of the fastest-growing opportunities in the security sector is the ability to monitor the elderly. With the rising costs of healthcare and the increase in innovative monitoring

capabilities, technologies are enabling loved ones to live in their own homes longer. These technologies include mobile PERS options for personal emergency response; sensors that alert when someone has fallen out of a bed or wheelchair; motion sensors that alert when they do not sense motion after a certain amount of time; contact sensors

that can alert when a medicine cabinet is opened; and more – and they are all fairly simple additions to enhance an existing security system.



IoT Healthcare Sensor Revenues Grow Globally

From monitoring and diagnostics to delivery methods, Internet of Things (IoT) sensors in healthcare combine sensor output and communications to provide functions that were considered conceptual, until recently.

IoT sensors in healthcare enable medical equipment to accumulate and share data with the cloud as well as each other, in order to facilitate the accumulation of data that is analysed with accuracy at breakneck speeds. IoT sensors in healthcare are wearable, cloud-based, or device embedded. With advances in IoT sensors in healthcare and healthcare IT, the industry now includes a dynamic collection of patient data in order to foster diagnostics and preventive care, and even measure the probable outcome of the preventive treatment.

Patient monitoring applications of IoT sensors in healthcare include IoT-enabled sensors integrated in healthcare equipment that monitor the condition of the patient during and after a surgery or a treatment. Such sensors also enable remote monitoring of patients. Diagnostics-based IoT sensors in healthcare are integrated in automated and network connected instrument guidance and measurement sensors, usually used during minor as well as major surgical treatments.

IoT sensors in healthcare are integrated in medical devices such as automatic medication dispensers in hospitals to enhance efficiency. Such sensors are also used to



market was valued at US\$2,208.9 million (€2,007.1 million) in 2017 and is expected to expand at a CAGR of 12.2% during the forecast period (2018–2026). The demand for IoT sensors in healthcare is expected to be driven by improvements in patient engagement, increased accuracy in data analysis, enhanced disease management and treatment results, and reduction in treatment costs.

monitor the medicinal cold storage in warehouses and well-funded drug stores with storage spaces. Other applications of IoT sensors in healthcare market include IoT-enabled sensing offered by wearable devices. IoT sensors in healthcare are also integrated in mobility devices for the safety and security of physically challenged patients.

Well-funded pathology laboratories, makeshift laboratories and clinics, dispensaries, and drug stores are some other IoT sensors in healthcare end users that integrate healthcare IoT sensors into their workspaces, in order to increase efficiency and offer better services and facilities.

Global IoT Sensors In Healthcare Market: Forecast

The global IoT sensors in healthcare

The global IoT sensors in healthcare market is categorised on the basis of application, end user, and region. On the basis of application, the IoT sensors in healthcare market is segmented into patient monitoring, diagnostics, clinical efficiency, and other applications.

The patient monitoring segment of the IoT sensors in healthcare market is expected to register a CAGR of 13.5% during the forecast period. By end user, the global IoT sensors in healthcare market is segmented into hospitals, CROs, rehabilitation centres, and other end users.

Among the regions, North America was the largest market in the IoT sensors in healthcare market, which accounted for over 21.0% of market share in 2017. Also, the demand for IoT sensors in healthcare is increasing in the market in SE Asia, excluding China and Japan.

How To Protect Yourself From The Siren Song Of Healthcare IoT

IoT promises to transform healthcare, delivering better care to more people. But there are significant risks. Just imagine the risks associated with connected ingestibles. When revolutionising the healthcare industry, we must remember to align our priorities around the immortal words of Hippocrates' oath: "First, do no harm." Innovate with care.

By Kristina Podnar, Digital Policy Consultant at NativeTrust Consulting, LLC

When I attend technology conferences lately, I find myself flashing back to the heady days of the early 1990s, when the internet was the final frontier, and anything was possible. After a while, of course, we got smacked on the nose by reality and started asking those "but what about..." questions that make product development less fun, but more effective (and, ultimately, more profitable).

Today, the Internet of Things (IoT) is in much the same place. Connected devices are transforming the world in ways we could barely have imagined back in the 1990s. Here's a short sampling of how IoT is already changing industries and lives (Hint: Alexa and Google Assistant are still riding with training wheels). I've noticed that the greatest excitement is focused on an industry that affects each and every one of us: healthcare.





IoT And The Bright New Future Of Healthcare

IoT is already improving care and allowing it to be delivered to more people. People in rural areas, for instance, can avoid long and expensive trips to a medical centre. ER visits are reduced when doctors can monitor patients' vital signs remotely.

And we're just getting started. It's an exciting time. It's no wonder that many entrepreneurial minds are gearing up to participate. Nonetheless, I encourage everyone from developers to healthcare providers (and consumers, too, for that matter) to stop for a moment and remember the words uttered by Hippocrates and immortalised in the oath named in his honour: "First, do no harm."

What Harms Could Stem From Healthcare IoT?

It's a little thing called "unintended consequences." They tend to pop up when we get so excited about our ideas that we don't stop and think about the possible downsides. And the healthcare IoT is full of them. That doesn't mean we shouldn't strive for innovations that make people's lives better; it just means that, before we get too far along in the development phase, we should ask ourselves, "What could go wrong?"

Let's look at one small slice of the healthcare IoT pie: ingestibles. Doctors at the University of Minnesota Health and Fairview Health recently announced that they're treating a small group of cancer patients with "digital medicine": a chemotherapy pill that includes a sensor to let patients and their doctors monitor their dosage—to make sure they're taking their medicine when they're supposed to.

That sounds like a good thing, right? Cancer is nothing to mess around with and complying with a treatment protocol is important. In fact, there are many conditions that could benefit from such real-time feedback. The Centers for Disease Control and Prevention (CDC) estimates that 20 percent of the 3.8 billion prescriptions written in the U.S. each year are never filled. Of those that are filled, half are taken incorrectly, especially when it comes to timing.

The cost of medical noncompliance is shocking. A report in the *Annals of Internal Medicine* estimates that prescription noncompliance costs the American healthcare system more than \$280 billion per year and is responsible for about 125,000 deaths.

Looking at those numbers, it's hard to argue that ingestibles that monitor compliance would have a downside. But, going back to the, "First, do no harm" mandate, developers and health care providers would be wise to take a closer look. How could such products cause harm? Let's start with these.

Security Risks

One of the biggest concerns developers have about IoT is weak security. A large part of the problem stems from the millions of connected household devices. 15 percent of all IoT device owners never bother to change the default password. Even somewhat competent hackers can use a mere five username/password combinations to access an astonishing number of DVRs, security cameras, and yes, even washing machines.

Now extend that line of thought to connected devices people carry around inside of their bodies. Health information is considered to be some of the most personal data there is. If those ingestible devices aren't properly secured, could people unknowingly be broadcasting their health status (not to mention all of the other personal data related to it) everywhere they go?

Takeaway

If you're going to develop ingestible IoT devices, don't skimp on security, from collection and transmission to storage and accessibility. The risks to consumer privacy and to your organisation should a breach occur can't be underestimated. (And I strongly encourage you to include your legal team in all of the conversations we'll cover here.)



Privacy Concerns

I would expect most developers to understand that any connected healthcare device would be subject to HIPAA standards. The problem is that we haven't figured out exactly what that means when it comes to things like ingestibles.

- **Who owns the device?** The manufacturer, the doctor, the healthcare system, the insurance company, or the person whose body it's in? And, if the manufacturer and/or doctor retain ownership, can they retrieve it at will, even if that means forcing a person to undergo an unwanted medical procedure? How would that be enforced? Through the courts?
- **What about the data on the device?** Regulations like the HIPAA and the GDPR suggest that the data would belong to the individual. So how would that work when it comes to gaining consent? Will your Terms of Service state that you can use all of the information for any purpose? Or will you need to get separate consent for each possible use of the data? Will you need to obtain renewed consent on a regular schedule?

And then there's the device itself. Will personal data be stored on the device? If so, can it be erased or deleted remotely, or will it require a medical procedure? Medical device risks are alarming, but they can be mitigated.

Takeaway

Early in the development process, brainstorm as many privacy scenarios as you can come up with, and develop a policy for each of them.

Maintenance

Will the device need regular maintenance? If so, will it require the patient's participation? In that case, you'll need to get that consent before the device is ever ingested. And what if it malfunctions? Can it stay inside the patient forever, or can it cause harm? If it does cause harm, who is liable? And who is responsible for retrieving the device and treating any damage it caused?

Takeaway

Meet with your legal team to discuss liability and risk before you invest too much money in a device that may be too risky to use.

Agency and Autonomy

What happens if the ingested device reports that the patient is not taking medication as prescribed? Does it trigger a phone call from the doctor or pharmacy, possibly counselling the patient on how important it is to take the

medication on the right schedule? What if the patient still doesn't comply? Current competency laws would probably apply to issues of whether a patient can refuse treatment, but could insurance companies use proof of noncompliance to withhold coverage, or even to deny payment on life insurance policies?

Takeaway

"Who decides whether to force a patient to undergo unwanted treatment?"

"Who decides whether to report this information to insurance companies?"

These are non-trivial questions. In fact, they're mind-boggling questions to discuss in detail with your lawyers at the very beginning of the development process, not when you've already got millions of dollars invested.

The Problem Of Unintended Use

Now that we've covered the technical and legal issues, it's time to fire up your imagination. This is the point where you try to think of every possible way people could use—or misuse—your device, decide what your position should be, and write a digital policy to address it. Because if there's one thing that history has shown us, it's that consumers are ingenious when it comes to using products in ways their developers never intended.

- Long before DIYers began using it to loosen stubborn bolts and hinges, WD-40 was designed to keep standing water from causing corrosion on nuclear missiles.
- Play-Doh was invented to clean wallpaper. Legend has it that some Cincinnati pre-schoolers found a stash and used it to make Christmas ornaments.

- Rogaine, the go-to answer to hair loss, was originally used as a treatment for high blood pressure.

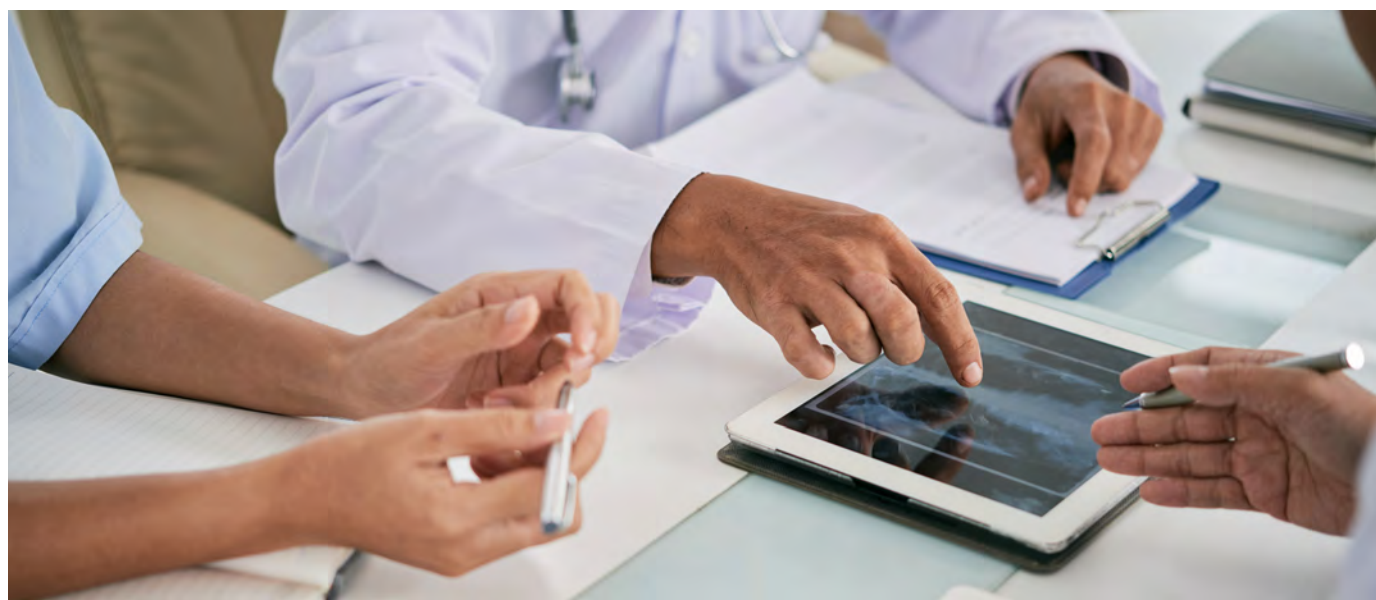
Unfortunately, not all consumer adaptations are quite so benevolent, as evidenced by product warning labels, like the label on a Dremel tool proclaiming that it's "not to be used as a dental drill." Or the Superman costume that warns it doesn't actually endow the wearer with superpowers or the ability to fly.

When it comes to ingestibles, however, concerns about unintended use are more about potential abuse of power. For example, once upon a time, police departments installed breathalysers in the cars of people convicted of drunk driving. They had to breathe into it and get a passing reading before the car would start.

Ingestible IoT devices could be used the same way. Police departments could give offenders the choice of losing their license or ingesting a device that would monitor their blood alcohol level. If the level were too high, the device could alert police and/or disable the car. Whether or not you would want your device used that way merits some serious discussion—and again, it should take place early in the development process.

Finally, Innovate With Care

On that note, I'll let you take your burst bubbles and go back to your drawing boards. But it's not my intention to discourage innovation in healthcare IoT. Far from it: I can't wait to see what all of the ingenious entrepreneurs out there come up with, and how your inventions will improve healthcare for all. I just encourage you to take the time now to ask yourself all of those "What could go wrong?" questions. I know it's not fun, but it would be a lot worse a few million dollars down the road!



How Smart Cities Improve Accessibility For The Elderly

Smart technology can help make a city more accessible for the elderly and disabled, enabling them to live independently.

One of the unsung benefits of smart cities may be their ability to help elderly people age in their own homes. There are many benefits of smart healthcare technology for elderly people. Smart cities can expand that caring technology to encompass a whole city.

Smart technology can also help make a city more accessible for people of any age and enable them to live independently and make the most of the benefits of city living.

An Aging And Urbanising Population

Many developed countries have an aging population. Ensuring that people can live full, happy, independent lives for as long as possible while coping with the challenges of an

increased aging population will be one of the most important tasks of the next few years.

In many parts of the world, baby boomers who left cities for the suburbs when they started families are now returning to urban centres. Many of the things that make cities appealing to younger generations, such as walkability, easy access to amenities, and opportunities to socialise, are also appealing to an older generation. We have a generation who are retiring while still in good health and many of them are seizing the opportunity to downsize to an apartment in the city.

Cities can be great places to age. Walkable city neighbourhoods make it easier to stay active, and medical care is close by if it's needed. Adaptations to the cityscape,





with the help of smart technology, can improve this experience further.

Elizabeth Burton, professor of sustainable building design and wellbeing at Warwick University, says, “There is a recognition now that as people age and their mobility reduces, they may no longer be able to drive, and their world shrinks; it is therefore much better to live closer to amenities in a higher density of people.”

Smart Cities For Aging Population

Helsinki, the capital of Finland, has been pioneering many interesting ideas about how to make the city more liveable.

One of their innovations is the mobile GPS app BlindSquare. The app helps blind and visually impaired people to navigate the city by describing their environment, announcing points of interest and street intersections, and giving them directions. It's easy to see how this type of fantastic innovation could help someone to live an independent, fulfilling life.

Tilberg, in the Netherlands, has been trialing a scheme where an app gives pedestrians with restricted mobility extra time to navigate pedestrian crossings. A sensor in the smart traffic light monitors the pavement, and if it senses someone with the special app installed, then the timing of the light is adjusted.

Using IoT Applications To Extend The Reach Of Healthcare

Barcelona is one of the world's leading smart cities in many areas, and its approach to elder care is no exception. Barcelona has introduced several schemes to make life better for its older residents.

In 2014, the city launched an app-based program to combat loneliness and social isolation amongst elderly people. They also proactively check on elderly and disabled citizens by utilising sensor technology as part of their Telecare service.

Seoul, in South Korea, has a similar smart city initiative with its U-healthcare service, which assists the elderly and disabled by providing medical consultation and telehealth check-ups.

Making Smart Cities Work For The Elderly

The key to making smart cities work for the elderly is for planners to put themselves in these people's shoes. Able-bodied city planners don't always recognise the elements of a city that may be challenging for someone else. Simple things such as uneven sidewalks or a lack of benches can make a city difficult to navigate.

Ideally, elderly and mobility-impaired people would be invited to take part in the planning process to ensure their needs are properly understood and cared for.

Another key aspect is to ensure that any deployed IoT applications are intuitive and easy to use so they're invisible. In Tilburg, urban planners struggled to find participants to trial the app, as potential users were wary of new technology. We must ensure the technology is simple to use and not seen as intimidating or complicated.



Project UFOund: Improving Hospital Logistics With IoT

Not knowing where things are can be inconvenient at best. In hospitals, not having wheelchairs, beds, and infusion pumps available at the right time can impede the required daily care.

By Liam van Koert, IoT Now

University Medical Centre Utrecht initiated the pilot project UFOund to tackle this problem in a user experience centre. They first tagged their equipment and connected it to a mesh network. Then they gave nurses and technical staff real-time information on the whereabouts of equipment. Better yet, they can 'beep' whatever they need with the push of a button.

It is not often that an opportunity, such as the one at the Children's Hospital in Utrecht, presents itself. But as the ward, which owes its name to the ample, cheerfully painted green frogs on the walls, is due for some serious renovation work, UFOund's Project Manager, Wiko Lamain and Clinical Informatician, Thijs Dijkgraaf, have turned the Second floor into a playground of their own. Having installed network 'anchors' and tracking tags, they can freely experiment with moving beds and pumps around and check various set-ups for accuracy and robustness, without interfering with daily hospital logistics.

They have also equipped a dedicated information centre which people from all over the world can visit to see what



they are up to. Hospital logistics are complicated everywhere. And UMC's novel IoT-based approach towards tracking & tracing, amongst other things, has received the medical community's attention.

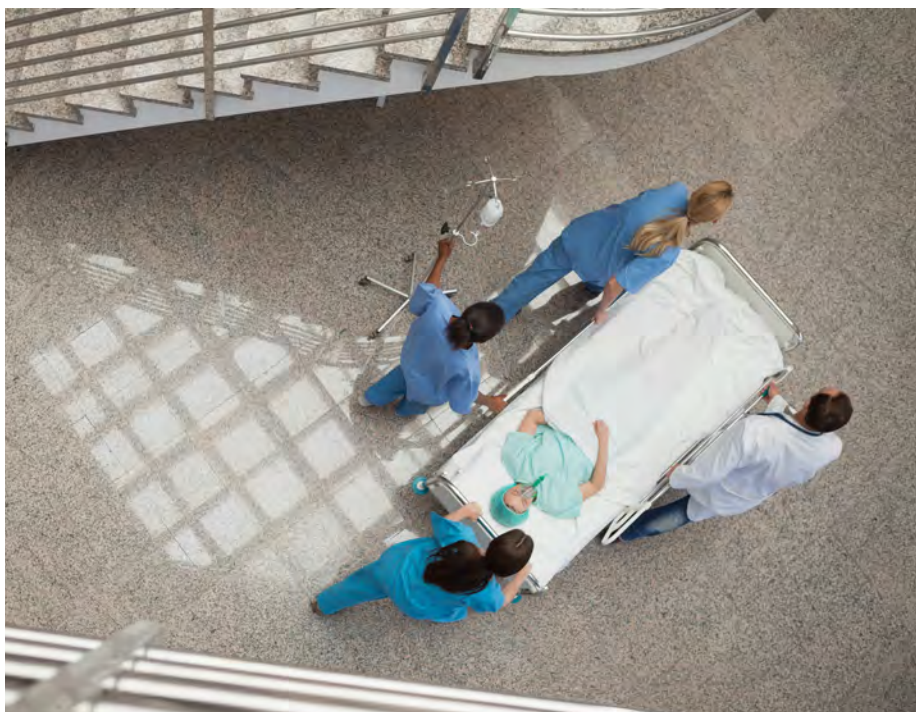
Processes First

"UFOund delivers the fundamentals for the MATriX project which aims at improving the quality of care provided in UMC Utrecht for both patients and staff" by improving the availability and employability of medical equipment, explains Lamain, who has been connecting lots of possible IoT dots for UMC for almost a year now.

"One of the things we try to achieve with the project is to better align workflow processes with the standard equipment used by our staff to nurse patients on a daily basis. We do so by first looking at our current processes, and then seek ways to improve them. Secondly, we investigate new technological opportunities that have arisen to support them." According to Lamain – like in many other fields – hospitals nowadays face having to provide higher quality care for less money, with fewer people.

Black Hole

In the search for bottlenecks to eliminate, UMC Utrecht found that not having immediate access to standard equipment was an unnecessary hindrance that could in



theory 'quite easily' be dealt with. Not knowing where beds, wheelchairs or infusion pumps are when you need them? It happens more often than one might think.

A wheelchair might be displaced or borrowed by a colleague for an emergency. Maybe a bed is broken, and it has been sent to the technical staff for repair. Whatever the reason, too much valuable time is wasted in the searches that inevitably follow.

Lamain comments, "When delving deep in the whereabouts of hospital equipment, you'll find that you might think you know where things are, but in many cases you actually

don't. Now you could – for improved tracking and tracing – introduce a system where all equipment is dispatched from a central location. Here you can check the equipment's technical status, plan maintenance and keep stock of the inventory in general. But you don't want nurses to walk a mile and a half every time they need something. They have patients to take care of.

Improved Patient Experience

There is, according to Lamain, a lot to be gained by using such a system, and not just from a logistics perspective. Patients will experience higher quality care due to more personal hands-on time from nurses and





smoother transitions from one ward to another. “One of the bottlenecks when moving patients is getting them hooked up to the right infusion pump. Every department has its own type, with its own settings. This results in patients having to switch pumps multiple times when going in and coming out of surgery. Using IoT for getting the right pumps at the right place at the right time will help to significantly improve the patient experience. And who knows what future IoT developments will bring in terms of negating settings and functionality, so that switching pumps can be a thing of the past altogether.”

IoT Playground

Finding the right IoT technology for project UFOund was no easy feat. There are ample different technologies to choose from, each with their own plusses and minuses. You can use active or passive RFID tags, barcodes, QR codes, and vision, to name just a few.

In terms of visibility, how accurate are these different methods? You can place scanners in doorways, so you know where things are at room level. You could also add cameras with image recognition software to know the exact position, but alongside the privacy issues, you would of course be limited to the line of sight.

When considering the price tag, passive RFID might seem the more affordable option, but the reading equipment is expensive. A better method could be using active – battery-powered – tags that send a signal to a mesh network. By measuring the distance between the tag and a minimum of two nodes, you can calculate the exact position using

triangulation. But how precise is exact? And do the high electromagnetic frequencies produced by the tags interfere with hospital equipment? How often should I send a position signal to the network for the logistic applications to run smoothly? How much data does this generate? How do I handle this? And what does this mean for the battery life of my tags?

These are just a few questions that Lamain and his team sought answers to. And they fortunately had an entire ward to use as an IoT playground to come up with some promising results.

Vast Ecosystem

One of these results is a robust mesh network that uses Wirepas for communication between the network nodes. Originally researched by Tampere University of Technology in Finland, this network technology is self-organising and thus always up and running. Also, it uses very little energy to do so.

“This mesh network is great for a wide variety of applications, hospital logistics being one of them,” Dennis van Doorn, marketing manager, Wireless Solutions at Fujitsu elaborates, while checking if everything is online. “Different nodes – used in this set-up include the mobile tags, sensors (environment monitoring such as temperature and CO₂, and fridge temperature monitoring) but also fixed anchor nodes – automatically connect with one another. Choosing the best communication channel, required signal strength and the best route for the data is a unique feature of this technology.

Smart Lighting And Switches

The large number of nodes that need to be installed and the power requirements that come along with it can be a challenge in mesh networking. However, as Sytze Terpstra from smart lighting provider Ingy explains, in the case of the UFOund project another novel idea provided a scalable solution that would not only address power requirements but would also fully support future IoT applications.

One of these applications is the integration of energy-harvesting wireless switches from EnOcean. The beauty of these is that no power is required at all. The energy induced by pressing the button is enough to switch the light or make a 'call' for assistance, a bed, or whatever function you want to use it for. And, as an added bonus, the lighting offers extra functionality such as daylight compensation, smart grouping and lighting plans based on presence or personal preferences. The presence sensor provides occupancy data which is processed and displayed in the GOOEE portal, which also catches the environmental sensor data such as air quality.

Tracking Platform

Another contributor that eagerly pushes around beds and pumps alike, while tracking them with his laptop via several especially developed applications, is Christian Sveistrup from Systematic. The Denmark-based firm that he works for specialises in decision-making software and has developed a comprehensive eHealth suite that forms the basis of a custom-made and role-based tracking solution for UMC Utrecht.

Sveistrup explains, "We use the longitude and latitude data we receive from the Wirepas tags for several applications. One is a viewer that visualises all the connected equipment on top of a floorplan. We also include additional information on the assets. Based on one's role, the user can thus see where the available beds or pumps that need servicing are located. General information can be shown on large screens, user-specific information on a smartphone or tablet. We can also add tasks and alarms in the form of notifications."

Indoor Navigation

Guiding patients and staff is another significant challenge in large hospitals, such as the UMC Utrecht. As navigation and wayfinding are currently offered through photo-based wayfinding, in this project other more dynamic methods have been introduced using the beaconing functionality within the Wirepas Mesh.

Nodes are able to transmit standard Bluetooth beacon messages, which are used in Esri's ArcGIS Indoors solution for indoor mapping and navigation. The ArcGIS Indoors

mobile application offers state of the art bluedot indoor positioning, wayfinding and turn-by-turn navigation. This enables the user to get accurate positioning in real-time on their mobile phone, find points of interest and people and navigate to them.

Data-driven Future

Taking it one step further, Systematic has also developed tools to optimise the patient flow. Here, besides the availability of assets, they also take into account elements like health and patient safety. Sveistrup: "This kind of optimisation involves complex data science that goes beyond your every-day statistical analysis. But when collaborating with some hospitals and R&D facilities in Denmark, it is amazing what you can achieve with hospital IoT. This, of course, lies way beyond the scope of project UFOund, but they do now have technology available that enables these kinds of use cases in the future."

Wirepas' eco-system partners are also working on this request, Dennis van Doorn explains, "With such an eco-system of very skilled partners we are able to cover a broad range of projects. By composing IoT components with the ability to operate together we can cover nearly any request."

Whether or not IoT projects, such as UFOund or the silent medical alarm study, will see a UMC wide roll-out is up to the board to decide. Lamain's playground findings will be up for review in the second half of this year.



3 Ways Video Technology Can Improve Patient Safety In Healthcare

In the world of healthcare, patient safety and well-being are primary concerns. And while hospitals and healthcare facilities have hundreds of resources available at their disposal, video has quickly become one of the most effective and trusted tools.

By Frank Landman, readwrite.com

All five of our human senses are valuable and useful. As anyone who's struggled with hearing or speaking knows, it's challenging to go through life when you don't have all of the same sensory strengths as your peers. Even having a bad sense of taste/smell or isolated numbness that makes it difficult to feel things is a big challenge. But there's arguably nothing more limiting and challenging than a lack of vision.

Eyes have been called the windows to the soul. They have the ability to both communicate information and relay information to the brain. Whereas most mammals have a strong sense of smell that allows them to collect information about their environment, humans are fairly limited in this capacity. It comes down to our ability to see.

It's been said that the human brain processes visual content

60,000-times faster than text, and that visual content makes up 93 percent of all human communication. In other words, it's a big deal.

As powerful as video is, it's also highly appealing. There's something satisfying about watching video. Most people would much prefer to be entertained with video than they would by reading or listening to another form of content. There's something magnetic about it that continually draws us in.

Then there's the utility of video. It can be utilised in so many different ways. Video can be used to monitor, educate, entertain, and communicate. And as the healthcare industry evolves, it's this aspect of video that's proving to be most useful for doctors, healthcare educators, hospital administrators, and other professionals in the field.

Three Specific Ways Video Is Improving Patient Safety

Doctors, nurses, and healthcare administrators have dozens of responsibilities. However, it could be argued that no single responsibility holds more weight than that of





patient safety. Without the proper safety systems and processes in place, nothing else matters. And the healthcare industry's growing commitment to video reveals this to be true.

There are numerous examples of ways in which video is improving patient

safety, but let's zoom in and look at three specific areas of application that are most intriguing.

1. Preventing Patient Falls

It's estimated that between 700,000 and 1 million Americans fall in a hospital setting each year. More than

30 percent of these falls result in an injury that requires further treatment and/or prolonged hospital stays. The average cost associated with these injuries is \$14,000. Beyond the patients themselves, these falls result in an increased risk of litigation for healthcare facilities. They also reduce patient satisfaction and create unnecessary friction for all parties involved.

Traditionally, the only way to reduce the number of patient falls has been to increase caregiver involvement. But as you can guess, this is an expensive investment that requires hospitals to increase staffing and payroll. And while physical caregiver involvement will always be necessary, many hospitals are discovering that remote monitoring of patients via video surveillance technology is much more practical for patients and cost-effective for the organisation.

The University of Maryland Medical System (UMMS) has been the leader in this charge. They've implemented a system by which observation





technicians located in a building near the hospital watch large, split screen monitors with up to 10 video feeds showing at once. The patients are spread across six different hospitals in the area. In addition to those who are considered risks for falling, the video feeds also follow those who are being watched for suicide behaviour or risk of seizure.

When the observer notices something abnormal, she engages the patient via a two-way communication device, while simultaneously speed dialling a nurse to show up at the scene. If the patient doesn't respond right away, an alarm is sounded.

Marc T. Zubrow, M.D., the system vice president for telemedicine at UMMS, reports video monitoring has saved the system more than \$1 million in the first year of operation alone. But even more than saving money, it's saved lives. Not only does the video surveillance prevent falls, but it allows doctors to respond much faster after falls occur. And in a business where minutes can mean the difference between life and death, this is a significant development.

2. Training Healthcare Professionals

There are few industries where training is more important to the integrity of

the job than in healthcare. If doctors, nurses, and other staff members aren't properly equipped to do their jobs, the consequences can be severe. In some cases, patients' lives are on the line.

Traditionally, medical student training has been hands-on. However, over the past few years, medical professionals have become increasingly concerned about the safety of patients during these trainings. (Morally, we have to ask the question: Should patient safety be compromised at the expense of teaching students how to perform

certain tasks?) As a result of these concerns, we've seen an increase in the role of simulation learning.

With technology like VALT by Intelligent Video Solutions—which uses a video recording system to train and analyse medical students in simulated settings—learning doesn't have to come at the expense of an actual patient's health and well-being. Mistakes can be made, lessons learned, and experience acquired.

Then there are the ways in which augmented reality (AR) is being used to help doctors and surgeons practice complicated procedures in real-time. Virtual simulations, which were once rudimentary and ineffective, now have an added layer of realism. Doctors have the chance to actually physically feel what it's like to perform a procedure. The hope is that these technologies will continue to improve, which will lead to doctors and surgeons who are better prepared to deal with a variety of situations.

3. Improving Telemedicine

Telemedicine, also known as telehealth, has taken a long path toward maturation. A decade ago, most people would have suggested that the industry would be further



along than it is right now. But due to a combination of patient resistance and technological inefficiencies, telemedicine has lagged behind. Evolving video technology is hoping to change this.

To date, the biggest problem with telehealth is that patients don't feel like they're getting as much value as they receive when they attend an in-person visit. Part of this has to do with the fact that they aren't always able to interact with doctors and nurses in a face-to-face manner. (Many telehealth services are administered via phone, email, or online chat.) But as video technology improves and the ability to stream content in real-time becomes more cost-effective and seamless, this is no longer the case.

Virtual visits are more popular than ever in situations where patients simply need to describe symptoms and get a prescription or professional medical opinion. Cases of the common colds, viruses, and the flu are perfectly suited for video. By staying home, patients lower the risk of spreading their germs and doctors are able to see more patients.

As video makes telehealth more practical, we'll see fewer instances of patients not seeking care in situations where they truly need a medical opinion. By removing the inconvenience of getting in the car, driving to the doctor, sitting in the waiting room, being seen, and driving back home, patients are more likely to seek out medical care and get the diagnosis or treatment they need to live happy and healthy lives.

Lights, Camera, Action

The utility of video is perfectly exemplified in the healthcare industry. From surveillance and monitoring to education and engagement, video is completely transforming patient safety for the better. But this is just the start. When we look back on the evolution of video in 25 or 30 years, we'll call 2019 the "early days."

Over the next three to five years, some pretty exciting things will happen with regards to video in the healthcare industry. Some of the biggest trends will be the ways in which video production is used to educate patients and give them better opportunities

to thrive (both inside and outside of formal healthcare settings).

Healthcare organisations—including insurance companies, physical therapists, and general practitioners—will add video production to their list of responsibilities and value-adding services. They'll begin to produce their own content that can be shared to their patients and customers in an effort to improve their ability to care for themselves at home.

Take physical therapy as an example. We'll see an increasing number of physical therapists produce their own video content to help patients perform exercises the correct way. Think of it like instructional yoga videos that you can find on YouTube today. Yet instead of being mass-produced video with general content, the video will be personalised to the individual patient. This will lead to better results and a more positive patient experience. Inevitably, the future will also hold some surprises. Video will take on forms and roles that we never thought possible – significantly improving patient safety and engagement along the way.



As Food Allergy Rates Grow, Connected Tech Creates Safety Net

Food allergy rates have been climbing over the last several years, and today as many as 15 million Americans have food allergies. This is a 50% increase between 1997 and 2011 and school-age children are especially vulnerable, disproportionately suffering from allergies to common foods like milk, wheat, peanuts, and soy.

By Frank Landman, readwrite.com

In order to decrease the prevalence of life-threatening reactions among young children, researchers are looking to smart technology devices that can detect allergens, alert caregivers, and keep vulnerable individuals safe.

Allergies, Intolerances, And Autoimmune Reactions

Though allergies are quite common, many people confuse allergies, food intolerances, and immunological reactions to food – and each is very different. For example, wheat allergies are different from Celiac disease, which is an autoimmune response triggered by the gluten protein found in wheat. In Celiac disease, the body attacks the lining of the colon, viewing the host body as a foreign substance.

Allergies are, by definition, an immune response to a harmless substance, explains iCliniq doctor and paediatric allergy specialist Parin Niranjambhai Parmar. The body attempts to attack that protein by releasing histamines. This can result in anaphylaxis, a multisystem reaction that can cause GI problems, skin reactions, and may result in airway obstruction and death. Intolerances, on the other hand, are often the result of pre-existing GI problems, such as irritable bowel syndrome (IBS), lack of certain digestive enzymes, as seen in lactose intolerance, or a sensitivity to certain compounds.

Though all of these reactions are biologically different, many of the devices designed to protect against allergies can also detect contamination that can trigger autoimmune reactions or symptoms of food intolerance. As these devices improve, they will likely have a significant customer base.



Detecting Contaminants

Gluten sensitivity is one of the most digestive complaints today, and many people eliminate gluten to manage unrelated health disorders, such as IBS, ADHD, autism, and skin issues. Unfortunately, 1 in 3 foods marked gluten-free actually contains some gluten contaminants. The risk of cross-contamination is also very high when dining out, even when kitchens take precautions to protect diners.



One device that can detect the presence of gluten is the Nima; a device brought to market by MIT researchers in 2016. Nima uses sensor technology to test a small piece of food and within two minutes can identify the presence of gluten. It can help protect patients with Celiac, wheat allergies, and varying levels of gluten sensitivity. A peanut-detecting version of Nima is also in development.

Diagnostics In Disguise

One of the difficulties of living with any serious health condition is that medical equipment can be hard to disguise and unsightly to wear. As children get older, they often reject medical alert bracelets, insulin pumps, and other tools meant to keep them safe. By disguising allergy detection technology



as a fashionable accessory, however, tweens and teens are more likely to take advantage of the tools available to them. The Allergy Amulet is a fashionable solution meant to encourage users to test their food for allergens. The device contains test strips and can be worn as a necklace or bracelet or stored in a special smartphone case and used to prevent accidental exposures. Originally designed to detect peanut proteins in concentrations as low as 1-2 ppm, the device is also being tested on common allergens such as egg, gluten, and shellfish.

Fast-Tracking Interventions

Finally, when it comes to food allergies in children, even those who are prepared to use their auto injectors can struggle to self-treat in a timely fashion. And if a trained adult isn't nearby, anaphylaxis can advance and be deadly. That's why one of the most important innovations in the allergy world is technology that helps children and teens get help before it's too late.



Harvard, working in partnership with the KeepSmilin4Abbie Foundation, has been researching a way to identify and speed treatment of anaphylaxis by creating a wearable auto injector that can measure early physiological changes and dose patients with epinephrine at the start of a reaction. With the growth of other auto-injection technology, such as that used in diabetes, this technology is primed for the market.

Food allergies can cause anxiety, limits on socialisation, and even bullying, but advanced tech can minimise the impact such reactions have on children's lives. Particularly as food allergy rates continue to rise, the importance of on the go testing and intervention will only become more important.

A Realistic Look At IoT In Healthcare

This article is an overview of the potentials and risk of using IoT in the healthcare and medical fields. Opportunities include elderly patient monitoring, increased access for rural patients, and increases in time efficiency for medical professionals and data collection. Risks include cybersecurity threats, energy brownouts, and HIPAA compliance.

**By Sarah Wolverton, a Communications Specialist
at mesothelioma.com**

Speculations of how flashy technological innovations like big data, artificial intelligence, and the Internet of Things (IoT) will affect the field of healthcare are at an all-time high. Separating hype from reality can give an indicator of where these fields are actually headed and how they might have the ability to change the face of healthcare forever.

IoT in healthcare has long been one of those technological innovations that seems like it could truly affect an entire field. For those unfamiliar with the Internet of Things in general, think of it more as the Internet of Everything. IoT devices are simply pieces of technology that have been connected to the internet with the purpose of sending, receiving or collecting information to enhance usability.

Mobile phones are perhaps the most well-known IoT innovations. Cell phones used to be explicitly for telecommunications, with little to no internet connections. Enter the smartphone, which now allows everyday people to access an entire world of information on a whim. Enter fitness devices like a heart rate monitor used to function independently of any internet capability, but now can be synced to computers and phones to gain better insights into performance during a workout.

How Is IoT Being Used In Healthcare?

Healthcare based applications of this technology are aiming to expand on doctors' ability to treat patients with quick and personalised care. This subset of IoT technology is known as the Internet of Medical Things, or IoMT. Data collection and

collation have always been hurdles for the medical field and having machines in charge of this task, rather than fallible humans, could prove to be a big step for new cures and better care.

Even the long-standing issue of having too much data to sort through and no singular place to collect it all could be solved with smart IoMT devices that store and tag data



correctly. Earmarking relevant data for analysis by humans or AI devices may be the breakthrough that the medical field needs to make sense of all its quantities of information. Diseases that have repelled a fool-proof cure may have finally met their match, too.

IoMT devices and medical technology using AI are being championed as the most effective ways to beat devastating diseases like cancer, and maybe even cure them. An illness like mesothelioma cancer, which often moves sneakily at first and then aggressively once full-blown, could be detected electronically by monitoring IoMT devices before a doctor could do the same. This could extend patient life expectancy considerably.

Beyond disease detection, diagnosis, management, and treatment, IoT could help reduce rising healthcare costs. With the aging baby boomer population, cost reduction is a big theme in healthcare today. Automating care and check-ups will reduce labour costs and time expenditures by physicians while providing people with a way to monitor their own health.

Where Is This Technology Taking Us?

These devices pose exciting possibilities for streamlining appointments, bringing care to rural patients, reducing non-essential visits to the doctor's office and monitoring the health of chronic and recovering patients.

For patients that live further away from medical professionals, visiting the doctor can be time-consuming,

expensive, and headache inducing. However, with the introduction of connected devices, telehealth appointments could be just as effective as an in-person visit, which could provide much-needed access to care for patients in rural locations.

Patients with chronic or serious diseases can also benefit from this advancing technology. For instance, diabetes patients constantly monitor their blood sugar, so IoMT devices could be lifesavers. Elderly patients who live alone could connect their monitoring devices to the internet, setting up alarms and emergency calls if their blood sugar drops too low.

Of course, this is only one scenario, but the potential for helping patients and doctors using this interconnectivity is huge. Allied Market Research predicted that by 2021, the worldwide value of IoT in healthcare will reach \$13.8 billion.

What Are The Risks Of IoT In Healthcare?

With any new technology comes certain threats and pain points, and IoT is no different. Threats like cybersecurity, dependence on technology, and HIPAA regulation compliance may make integration and adoption develop more slowly.

Medical records listed on connected systems, though ideally encrypted and consistently backed up to secure servers, could be targets for identity theft or medical fraud. For some hospitals and patients, updating to electronic records may not be enough of a payoff for the potential risk.

Worries over cybersecurity breaches extend to not only medical records but also to the devices themselves. Medical equipment that is used to keep someone alive, like a pacemaker, oxygen or a life support system, could be vulnerable to hacks if connected to the internet, leaving patients without a fighting chance.

HIPAA compliance currently states that hospitals are responsible for ensuring that all data is secured, controlled and scanned regularly for any security threats. However, even the securest of systems can be in danger of a breach and the stakes happen to be a lot higher in the case of a medical system or device being compromised.

The Future Of IoT In Healthcare

Altogether, IoT seems to be an exciting development in the medical field. With growing value and prospects to save money and lives, the positives outweigh the negatives. Risks mentioned above can be patched and continuously assessed to prevent any breaches or loss of machine functionality. Look forward to more news on IoMT advancements and usages to inform your own opinions and monitor the field.



How Facial Recognition Technology Threatens Basic Privacy Rights

As adoption of facial recognition systems continues to grow worldwide, there is increasing concern that this technology could undermine fundamental privacy rights and how it can be kept in check.

By Nicholas Fearn from ComputerWeekly

Surveillance and facial recognition technologies have become a common fixture in today's interconnected world over the past few years.

Whether monitoring people in airports, searching for wanted criminals, allowing users to unlock their phones or creating targeted marketing campaigns, adoption of this technology has become widespread and resulted in many useful applications. But it has also generated legitimate concerns around privacy and security.

In December 2018, for example, civil liberties group Big Brother Watch described citizens as "walking ID cards" citing research that found police use of facial recognition tools identified the wrong person nine times out of 10.

As worries that these systems threaten basic human threats to privacy continue to grow, there is increasing pressure on governments and organisations to introduce stricter rules to keep them in check.

Inaccurate Tech

Although the use of surveillance and facial recognition technology is widespread and always growing, these systems are still in their infancy and can often be inaccurate. Michael Drury, partner at BCL Solicitors, says the biggest problem is that they are "hit and miss" at best.

"Most people would applaud facial recognition technology if it prevents the commission of terrorist atrocities and other serious crimes. But that remains a very big 'if', and the

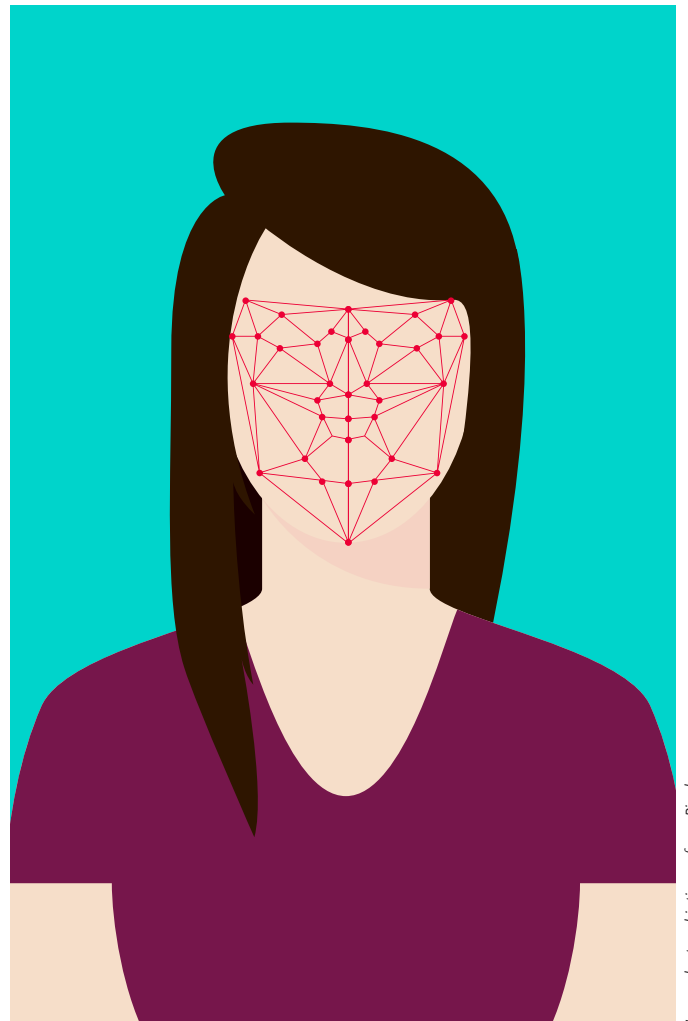


Image by teguhjati pras from Pixabay



potential benefits need to be weighed against the cost to us all of having our very beings recorded and those details held by the police," he says.

"We know it is better at recognising men than women, and Caucasians rather than other ethnic groups. The potential for misidentification of suspects and miscarriages of justice is one which should not be underestimated.

"Police and other law enforcement agencies should be wary of seeing new technologies as a panacea and worthy of use simply because the word 'digital' can be used to describe them."

Miju Han, director of product management at HackerOne, echoes similar concerns with regards to the reliability of these systems.

"Facial recognition technology has two major problems," says Han. "The first is that its accuracy is nowhere near 100%, meaning that employing the technology will result in many false positives. Few algorithms were trained on a truly representative sample, so facial recognition will disproportionately negatively affect different demographics.

"But even if we take the highest demographic accuracy today—which is around 99% for white males—and used the technology in a high-traffic area to attempt to identify known terrorists, for example, 1% of all passers-by would be incorrectly tracked, which would quickly add up to hundreds or thousands of errors a day.

"The second major problem is that users have not consented to being scanned. Going out in public cannot be a consent to be tracked. It is possible for an entity to use facial tracking to construct full location histories and profiles, albeit with a lot of errors. Your face is not a license plate."

Harming Privacy

When it comes to building a case for surveillance and facial recognition applications, it is often argued that they aid security. Steven Furnell, senior IEEE member and professor of information security at Plymouth University, believes that this can be problematic.

"Security and privacy are often mentioned in the same breath and even treated as somehow synonymous, but this is a very good example of how they can actually work in contradiction," he says.

"The use of face recognition in a surveillance context is presented as an attempt to improve security—which, of course, it can do—but is clearly occurring at a potential cost in terms of privacy.

"It has been claimed that face recognition technology is now societally acceptable because people are used to having it on their smartphones. However, the significant difference is that this is by their choice, and to protect their own assets. Plus, depending on the implementation, neither the biometric template nor the later facial samples are leaving their device.

Furnell argues that, in the implementations deployed in public spaces, the subjects are not consenting to the creation of templates nor the capture of samples.

"The data is being used for identification rather than authentication. As such, the nature of the usage is significantly dissimilar to the more readily accepted uses on a personal device," he says.

Comparitech privacy advocate Paul Bischoff says people need a way to opt out and that, without checks and regulation in place, face recognition could quickly get out of hand.

"Face recognition surveillance will probably grow more commonplace, especially in public venues such as transportation hubs and large events," he says. "It brings up an interesting discussion about the right to privacy and consent: do you have any right to privacy in a

public place? Up to now, most people would answer no.” But consider that even in a public place, you have a certain degree of anonymity in that the vast majority of people do not know who you are – assuming you’re not a public figure.

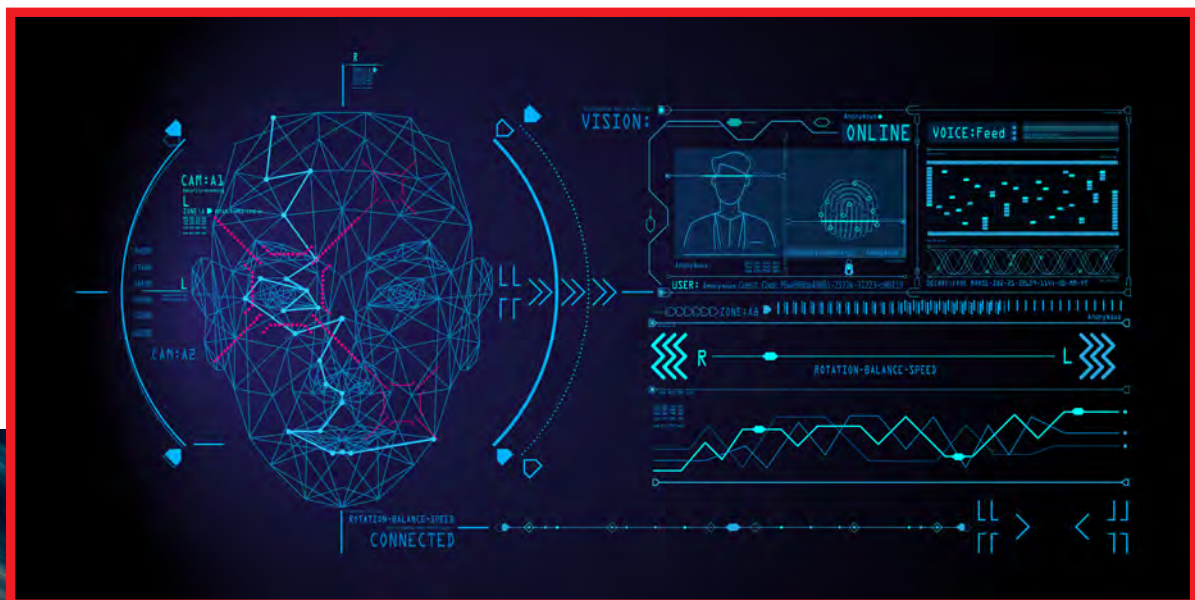
You can get on the subway without anyone recognising you. But if a security camera armed with face recognition identifies you, it can tie your physical identity to your digital identity, and it can do so without obtaining your consent first.

“People act differently when they know they’re being watched, and they act even more differently if the person watching them knows who they are. This can have a chilling effect on free speech and expression,” says Bischoff.

Clamping Down

With these threats in mind, some governments and organisations worldwide have begun implementing stricter rules and regulations to ensure such technologies are not abused. More recently, city officials in San Francisco voted eight-to-one to ban law enforcement from using facial recognition tools.

Joe Baguley, vice-president and chief technology officer of Europe, Middle East, and Africa (EMEA) at VMware, believes that the city of San Francisco is right to show caution in this case. As Drury and Han pointed out earlier, Baguley says the problem is that facial recognition software is not yet



sophisticated enough to positively benefit police and other public services.

Before these technologies can effectively assist with policing and surveillance, Baguley says the underpinning artificial intelligence (AI) algorithms need to be altered to ensure the software recognises people without any discriminatory bias. It is not just in the US where legal and regulatory challenges surrounding facial recognition technology are taking place.

In March, the UK's Science and Technology Committee warned that live facial recognition technology should not be deployed by British law enforcement until concerns around its effectiveness were resolved.

In June, a court in Cardiff concluded that rules governing facial recognition systems need to be tightened after a Welsh shopper launched a legal challenge when a South Wales Police camera took a picture of him.

Robert Brown, associate vice-president at Cognizant's Centre for the Future of Work, says these challenges herald a sea change in how much privacy we are willing to give up in the name of safety.

"On the one hand, it is a natural reaction to think, 'Good, facial recognition helped catch a bad guy,'" he says. "But then you wonder, 'How often can that 'eye in the sky' see me – and can I trust it?'"

Brown says that as we continue to see the rise of facial recognition as a means to keep us safe, we are going to have to navigate a thorny mix of standards, laws, regulations and ethics. "This means that we need consent of citizens—not digital-political overlords—to ultimately control who watches the watchers," he adds.

Mitigating The Risks

With facial recognition constantly gaining traction for a range of purposes, it is clear that more needs to be done to keep this technology in check.

"Principles such as storage limitation, data minimisation, and lawfulness, fairness and transparency apply to the processing of this data," says data privacy expert Tim Jackson, adding that there is no code of practice that currently applies to the processing of biometric data.

Despite the lack of a specific code of practice, there are a number of steps that need to be taken by companies that are developing or using this software.

"As we are talking about a high-risk processing activity, a data protection impact assessment must be carried out



before the processing begins," says Jackson, adding that the ICO provides detailed guidance on what form this assessment should take.

"This assessment will help the company identify the various risks that need to be mitigated, risks such as discrimination, unconscious bias, lack of transparency, and lack of proportionality, for example."

Jackson recommends ensuring that the development stage of any facial recognition software includes representation from different ethnicities and genders; ensuring individuals whose data are to be processed are made fully aware of this activity, what rights they have in relation to their data, and how to invoke these rights.

He adds that it should also apply strict retention periods to the collection of any data; apply confidentiality measures to the collection of any data; consider whether the scope of the facial recognition software could be reduced; seek the views of individuals before the processing begins to understand their concerns and adopt further measures if necessary.

Any facial recognition system should also consider whether there are alternative, less intrusive ways to achieve the same outcome; and create policies to govern the processing activity and to provide direction to staff, according to Jackson.

It seems the use of facial recognition technology is a double-edged sword. Although some people argue that these systems play an important role in fighting crime and assisting with other important tasks, they also present privacy challenges and risks.

As adoption increases, safeguards, laws and regulations will certainly need to be reviewed and revised to ensure consumers are protected and that this technology is not abused.

Making Sense Of Today's Security Camera Options

With so many choices available today, it's not always easy to understand which security cameras are best to fit your needs.

Reproduced from a Whitepaper by Vicon Security

IP-based surveillance cameras offer advanced functionalities that enhance the control and management of live and recorded video data, offering capabilities that were unthinkable only a decade ago. New technologies and camera designs are addressing a host of issues, including higher resolutions, wide angles, and different form factors.

Higher Resolutions

The appetite for higher resolution cameras, at lower price points, is ever growing. When does it make sense to pay for more megapixels? And what options exist for upgrading old analogue systems? Here are two camera categories that are making an impact.

1. Ultra HD

Just five years ago, 1080p cameras were state-of-the-art. Now, 4K cameras, which are the equivalent of four times the resolution of 1080p, are readily available, as well as cameras with even higher resolutions.

While dazzling 4K displays make sense for AV displays and digital signage, that level of detail is rarely used in live monitoring of security video. System operators typically view a matrix of cameras within the VMS interface, so



even if the workstation monitor is 4K, the screen is filled with many scaled down images. Think of paying to watch an IMAX movie on a screen the size of a 55-inch TV.

However, in the case of forensic investigation and the need to study recorded video, the investment in 4K cameras can really pay off.

The captured 4K image allows for a tremendous ability to zoom in and see details with a level of clarity not otherwise possible. It also provides video analytics engines with more data to work with, making tools like facial and license plate recognition more accurate and powerful.

There is a price premium attached to 4K cameras – and not just for the cameras themselves. The more megapixels in your video, the more bandwidth and storage space are required and the harder your display device must work to process the video. Various iterations of AVC/H.264 and HEVC/H.265 compression have helped to reduce file size and storage costs have generally fallen.

Even so, more megapixels are not always the better solution. Consider the field-of-view you need covered. There are plenty of applications where 4K cameras are worth the investment, like city surveillance, busy transit hubs and large casinos, but if a camera with

a lower resolution can clearly display the level of detail you need, there's no need to go any higher.

2. HD over Analog

For retrofit installations with an existing coax infrastructure and a customer who doesn't care about all the features that newer IP cameras can offer—they just want higher resolution than their old analogue cameras can provide—HD over analogue may be the way to go. These cameras can deliver 1080p high-definition video of the same high quality as IP cameras, and some DVR devices can directly accept their HD input. HD analogue can travel up to 1600 feet over coax. A key advantage of upgrading to HD over analogue is





that you do not have to swap out your entire CCTV system at once; focus first on placing HD cameras in high-risk areas or large, open spaces like parking lots, hallways and sales floors for better detailed footage.

But here's the catch. If you want to incorporate the video from these cameras into a professional grade network video management system, you'll need to use a video encoder to digitize and encode the video into a format that your software can process.

Depending on how your VMS solution handles licensing, HD over analogue can offer savings in camera licensing fees. Encoders often require only a single license, while offering the ability to connect as many as 16 cameras to the network.

Wide Angles

Security departments looking to reduce the number of cameras required to cover their buildings and properties have driven the demand for wider fields-of-view. Hemispheric cameras offer two different approaches. We'll also touch briefly on whether traditional PTZ cameras hold relevance in light of these new camera options.

1. Hemispheric

Hemispheric cameras, with their fisheye lenses, offer 360-degree vision. They are used in conjunction with dewarping software—either within the camera or VMS—to flatten the distortion caused by the lens. Video can be monitored as two panoramic 180° strips, quad views, or multiple custom views focusing on specific areas of interest.

When positioned well, hemispheric cameras can reduce or eliminate blind spots. For example, a single camera mounted on the ceiling at a hallway intersection within a school or office can provide simultaneous coverage of all four hallways, as well as an overhead view of the intersection itself. Other strong use cases include retail, warehouses, lobbies, parking

lots and manufacturing/industrial environments.

Hemispheric cameras are less expensive than multi-sensor cameras, less physically obtrusive, and perform well in indoor and outdoor applications. However, they generally do not perform as well as multi-sensor cameras in low light and variable lighting conditions.

2. PTZ

Although the optical zoom capabilities of traditional PTZ cameras are hard to match, many customers who use them will talk of instances where the camera was pointed the wrong way when an incident occurred. Multi-sensor and hemispheric fixed cameras offer the advantage of always recording the entire area of coverage, while providing a virtual pan and zoom experience that can be applied to both live and recorded video. The higher the camera's resolution, the closer it approximates true PTZ.

As higher megapixel fixed models have come down in price, the market for true PTZ cameras has continued to diminish. However, there are still instances where the power of high optical zoom is needed, and even a 20MP multi-sensor camera can't compete with the magnification offered by a 1080p PTZ dome with 20X optical zoom. If you compare the math, 1080p is the equivalent of 2MP, so at 20X zoom, it can provide twice the zooming effect of a 20MP fixed camera without pixilation.

In some scenarios, it makes sense to use both types of cameras simultaneously, as PTZ cameras work great for flexible wide-area surveillance and detailed monitoring. With a PTZ camera, you can control the pan/tilt/zoom functions to follow activity and zero in on specific individuals and objects within a scene. For example, in a commercial port, use of multi-sensor or hemispheric cameras can provide a cost-effective means to provide coverage of the docks, cranes, harbour traffic and all

other activity within the vicinity, while a few PTZs might be deployed to provide a view out to the horizon for live viewing, in case of an emergency. As the security industry turns its focus to megapixel, fixed, wide-angle cameras, it's important to still consider the strengths of PTZs and what they can deliver.

New Form Factors

Not so long ago, security cameras came in two form factors, box cameras and dome cameras. Bullets were an evolution of the "box." Now we're seeing a few more new options growing in popularity.



1. Turrets

The "turret" camera, or "eyeball camera" as it's referred to by some manufacturers, is now a widely available design.

Like domes, turrets can be mounted discretely either vertically or horizontally and are adjustable to achieve the required field-of-view. They are easier to manually position than domes because there is no covering to remove.

The shape of the unusual housing offers other benefits too. When used outdoors, the straight face of the turret design causes rain droplets to run off it more efficiently than on a dome. Moisture can get trapped inside a dome, causing it to fog up. Additionally, turret cameras are not subject to infrared (IR) "bounce," a problem inherent in the design of dome cameras equipped with IR illuminators,

in which dots of light reflect off the inside of the dome and are captured by the camera's sensor.

Turrets may not be a good choice if strong vandal protection is required – domes offer more ruggedized housing options. In addition, darkened or reflective domes can conceal the direction in which their camera lens is facing, making it difficult for criminals to actively avoid the camera's field-of-view. Turrets offer full transparency.

2. Micro Domes

As commercially available tiny, low-priced domes have made headway into the marketplace, manufacturers of professional grade security solutions have started offering more high-end cameras packaged in the small housings that customer's desire. New micro domes offer the higher resolution of their larger siblings, with features like vandal-proof and weather-proof housings, multi-streaming and sophisticated image processing capabilities. These professional level specifications provide justification to spend more than the rock-bottom prices of the consumer-grade micro domes, which are basically a webcam packaged in a cheap dome housing. Meant for discrete surveillance applications, the micro dome is perfect for a long hallway, corner of a room, or for an entrance of a building.

As more features are built into these tiny cameras, they will be used in applications where standard sized domes have traditionally dominated, offering a less obtrusive and superior aesthetic.

Conclusion

These are just a few of the benefits available from a new generation of security camera technologies available to today's end users. A deep analysis of each variable in an application should point to the type or types of solutions that can best accomplish the mission – at a total cost of ownership that isn't a budget breaker.

Leveraging The Biometrics Ecosystem To Improve Cybersecurity

The biometrics ecosystem is evolving at a rapid pace and providing incredible benefits to enterprises that adopt the technology, especially when these now-commonplace features are applied for cybersecurity.

By Bojan Simic Cofounder and CTO, HYPR

Although people are already familiar with using a thumbprint or facial recognition to unlock their mobile device or complete an online purchase with it, the real power of biometrics extends far beyond these simple features and experiences.

As massive data breaches spilling millions of user passwords and shared secrets become a familiar part of our everyday lives, so does the reality of malicious hackers leveraging these credentials to cause widespread damage. Due to the sheer number of compromised user credentials available from these spills, identity theft is at an all-time high, potential GDPR fines loom over many organisations, and there is an atmosphere of distrust.

This is where biometrics can provide an answer because these features we rely on for convenience can also have a ground-breaking impact on security and privacy. Providing that we follow a hard and fast rule -- that biometrics are combined with public-key cryptography.

In order to properly leverage biometrics, however, IT and security teams should first understand the key elements that make it such a powerful tool to combat today's ever-evolving threat landscape and, how to begin implementing it without requiring a complete overhaul of security infrastructure.

The Biometrics Ecosystem

One of the most powerful aspects of the biometrics ecosystem as it relates to cybersecurity is that it replaces the



shared "something you know" factor of user authentication with the difficult to reproduce "something you are" factor. Whereas passwords and shared secrets can be stolen and duplicated, every person's biometrics are completely unique.

The devices that match biometrics to their enrolled templates have grown in sophistication and are already in our hands. The vast majority of sensors on modern mobile devices have a 1/50,000 minimum false acceptance rate (FAR) which makes it extremely difficult to mimic a biometric template.

Using these sensors paired with standards-based authentication such as Fast Identity Online (FIDO) protocols that eliminates shared secrets creates significant friction for the bad actors who weaponise credentials for fraud through account takeover. It also disrupts a hacker's attack vector (and thus their economic model) as they can no longer focus on huge server stockpiles of user credentials and must instead go to individual devices to attempt to obtain a single user's credentials.

This shift makes it virtually impossible to have the mass credential breaches like the ones we are experiencing on an almost daily basis today.

Select A Use Case And A Secure Model

When launching a biometrics strategy, IT and security teams should look for areas where biometrics can have the greatest effect while creating the least amount of friction, and begin deploying the capabilities there. Oftentimes this is with internal facing applications that don't directly impact customers. Or, they can take the route of securing consumer-facing apps since biometrics are so popular with



their users and consumer devices with advanced capabilities are readily available.

Even the most forward-thinking organisations can balk at biometrics when they think it requires an unmanageable set of changes, such as the addition of special hardware, gutting of associated solutions or the taking on of unacceptable kinds of risk such as custodianship of biometrics.

However, the best way to implement biometrics into the security framework is through a deliberate and gradual process using a solution that is built upon mobile-centric FIDO standards. FIDO-based solutions are built to play nicely with security products already in place, and the strength of the standard ensures that users—not the enterprise—are the stewards of biometrics.

Make User Experience A Top Priority

Finally, despite all of the security benefits the biometrics ecosystem provides, if the user experience is clunky it will be difficult for users to adopt. The good news is that providing an easy-to-use, uniform experience for biometrics is rather simple due to the sophistication of today's mobile devices. Every employee already has a company or personal smartphone and experience using biometrics to unlock the phone make a payment.

The biometrics ecosystem provides incredible opportunity to create a more secure online world while building upon the experience smartphones have proven to deliver their users. Enterprises that want to roll out biometrics-based services today are poised to fully capitalise on it.

Thanks to the sophistication and ubiquity of the devices, and to the availability of solutions built upon open standards-based decentralised architectures, migrating to a true password-less state is within reach. Once it's deployed—even on a limited basis—my guess is that the enterprise will begin to see other areas for implementation across the enterprise.

Risk And Identity-defined Security Paramount As Attacks On Biometric Data Rise

The compromise of biometric data has dominated headlines of late, and it's an issue that isn't going away anytime soon.

By Jeff Wichman, Practice Director of Enterprise Incident Management at Optiv Security

While the idea of using fingerprints or facial recognition as a means of authentication might seem to be more secure than garden-variety passwords, biometric data is just that – data; and data can be stolen.

Unlike passwords, it's unchangeable data, which makes it potentially far more valuable. Against this backdrop, it makes complete sense that attackers would set their sights on this gold mine of data. Organisations are increasingly using biometric data for authentication and identification purposes, which introduces several new avenues of attack for cyber-criminals:

Motive: Infiltration Of Corporate Networks

Organisations have been struggling with preventing data breaches caused by weak passwords for decades, and the tech community has continually tried to help their efforts by introducing additional layers of authentication, such as geo-location data, tokens and, now, biometric data.

Attackers have figured out various ways to defeat each layer of the multi-authentication stack, and biometric data is no exception, thanks to data manipulation tactics. Once hackers get their hands on this data, they hold the proverbial “keys to

the kingdom” and can infiltrate corporate networks to steal assets and information that will result in financial gain.

Motive: Cyber Warfare

Adversaries, such as nation states, are increasingly targeting biometric data used for identification as part of their cyber warfare strategy. Additionally, facial recognition technology is making it easier and faster than ever to identify someone in public by their facial features alone. For individuals in government, law enforcement and the military, the impact



of a breach of this nature could be catastrophic – even life threatening.

The Necessity Of Biometric Data

Many organisations operate with an “outside-in” security model, where external threats and compliance mandates dictate security strategy and spend. In other words, they react to the latest threats by implementing the latest and greatest technology solution (in this case, using biometric data for multi-factor authentication and identification), without stopping to consider whether adding the technology in question is actually necessary to mitigate risk.

A better approach to security is, you guessed it, “inside-out,” where enterprise risk dictates security strategy and spend. In this world, the impact of using biometric data on enterprise risk would be the determining factor – will it make it harder for bad people to compromise identities and penetrate our systems? Or will it only add a new risk that could be expensive and time consuming to mitigate?

For example, in some cases, organisations may find that they need to leverage biometric data for multi-authentication to mitigate risk, and they may have an effective strategy for ensuring that the data is always encrypted and secure. In this case, biometrics might very well make an enterprise more secure and productive, since users won't have to do password resets or get locked out of systems they should have access to.

However, other companies may find that it makes more sense to strategically segment their networks and data, rather than add biometric-based authentication layers that make it harder for users to get onto a network in the first place. The security strategy for each company will be different, as each organisation has a unique risk profile.

The Age Of Identity-defined Security

In an age where digital transformation has made it impossible to build virtual walls around data, identity has become the new perimeter, and biometric identifiers now serve as a new type of access control. In this new world, organisations need to mature their identity and access management (IAM) programs to incorporate identity-centric security.

At a high level, identity-centric security is a concept that advances perimeter-based security by implementing next-generation IAM practices and integrating IAM more tightly



throughout the entire security program. The first step to achieving identity-defined security is to commit to it, and that means making a strategic investment in a programmatic approach to IAM.

Key access considerations include people who have access to personally identifiable information, biometric data, source code and intellectual property, human resources data, and so on.

Once this information is understood, you can move forward with basic controls such as access control, user lifecycle management and access governance. With these controls in place, you've set the foundation for identity-defined security and can move on to more advanced controls.

Biometrics is one of these advanced controls – and, as with everything else in security, technology should be considered from an enterprise-risk perspective. For example, if you haven't already implemented the “blocking and tackling” elements of IAM cited earlier, then there's not much point in implementing biometrics.

Which brings us back to our original question: Is the use of biometrics really necessary? To that question I can confidently say: maybe yes, maybe no. If you've done a good job at implementing identity-defined security in your organisation, then maybe biometrics could be useful for specific systems and data.

If you haven't done that, then it's likely biometrics qualifies as a “shiny object” that will only distract you from doing what you really should be doing: building a robust identity management program.

Mobile Biometric Authentication: The Advantages And Disadvantages

Mobile IT professionals must learn about the pros and cons of mobile biometric authentication before they implement fingerprint or face scan authentication factors.

By Robert Sheldon from TechTarget

In many ways, biometric authentication is superior to a traditional password due to its convenience and resistance to common attack vectors. But biometric authentication still faces its fair share of threats.

If a hacker gains access to a user's biometric data, that user can't reset their biometrics the way they might reset a compromised password. Malicious actors can also use fake mobile biometric input to spoof mobile devices.

Organisations that support and manage mobile devices should learn about biometric authentication advantages and disadvantages for enterprise mobility.

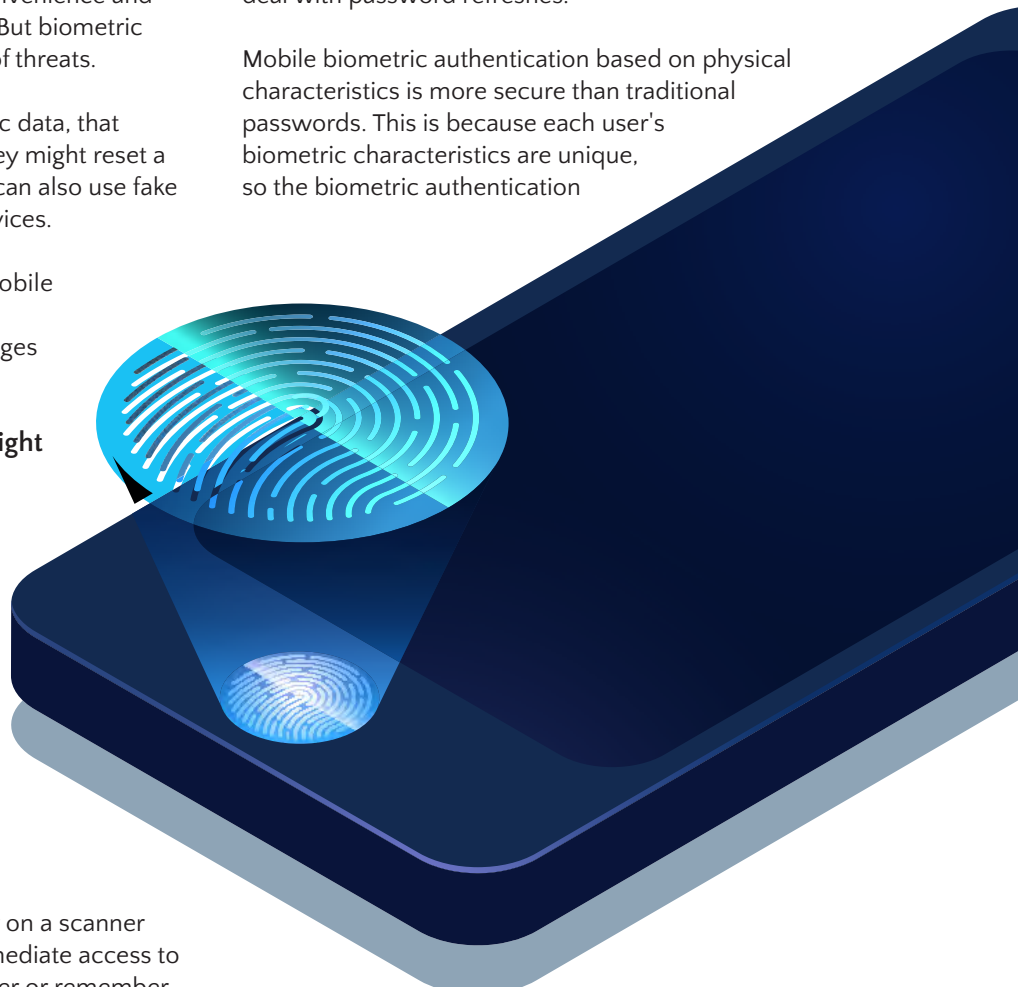
What Biometric Authentication Does Right

Biometric authentication is the process of verifying a user's identity based on unique physical characteristics, such as the user's retina, voice, fingerprint or facial features, and it presents a number of advantages. The most common approaches to mobile biometric authentication are fingerprint scanning and facial recognition. One of the biggest advantages to fingerprint and facial scans is the degree to which biometrics simplify authentication.

Mobile users only need to place their finger on a scanner or look at their device's camera to gain immediate access to the mobile device. They do not need to enter or remember

complex passwords and passcodes, nor do they need to deal with password refreshes.

Mobile biometric authentication based on physical characteristics is more secure than traditional passwords. This is because each user's biometric characteristics are unique, so the biometric authentication



factor provides a high degree of certainty that the individual logging onto the device is indeed the owner of the device.

Password-based authentication is notoriously flawed and hackable. Users can lose, forget or accidentally divulge their passwords, and hackers can steal or crack passwords. In contrast, biometric authentication makes it much more difficult to guess the authentication factor or trick users into revealing it. Additionally, users cannot forget biometric factors in the way they could a passcode.

Mobile biometrics come out ahead of other biometrics, as well, because the users' data is stored on the device and never transmitted across networks or collected on centralised servers -- two common criticisms of biometric authentication. Today's mobile devices also take important measures to protect the data on the device, such as using advanced encryption and isolation techniques.

Where Mobile Biometrics Can Go Wrong

Mobile biometric authentication is more convenient than passcodes, and mobile devices have several safeguards for biometric data. But these devices might still be vulnerable to significant risks. Hackers are continuously looking for ways to penetrate biometric defences.



There is a chance, for example, that hackers could break into iOS' Secure Enclave, the specially designed storage location that ensures biometric data never leaves the iOS device, and reverse-engineer the biometric file to access the data. The odds of a hacker accomplishing this feat might be slim, but no system can ensure indefinite immunity to all threats. Even if Android and iOS were able to guarantee such protections, there are other less direct risks to consider.

In 2015, for example, cybercriminals targeted the U.S. Office of Personnel Management and stole the fingerprints of 5.6 million current and former government employees. The hackers could come up with a way to use these fingerprints to target mobile devices that rely on fingerprint authentication. Initially, this type of attack might be limited to direct physical attacks that target the devices of specific individuals, such as high-profile users with access to sensitive data. At some point, however, the criminals might also figure out ways to spoof mobile

devices remotely, making it possible to hack them en masse.

In the same year that hackers targeted the Office of Personnel Management, researchers demonstrated how they could remotely steal fingerprints from Android devices and gain access to them. Although Google has since fixed this security hole, it demonstrates that mobile biometric hacking is hard to predict and difficult to prevent, especially if the would-be hackers are motivated enough.

Dangers Of Biometric Authentication For Mobile Devices

The advantages of biometric authentication are intuitive and somewhat obvious:

- Users don't have to remember passwords.
- Devices validate the user's identity with a simple gesture, such as placing a finger on a scanner.
- And it is extremely difficult for hackers to access biometric factors.

Biometric authentication for mobile devices makes it even more difficult for hackers to access these factors, because the biometric data is only stored locally.

Considering these benefits, biometric authentication for mobile devices sounds like an excellent approach for any organisation to take, but it may leave an organisation and its users susceptible to unique threats.

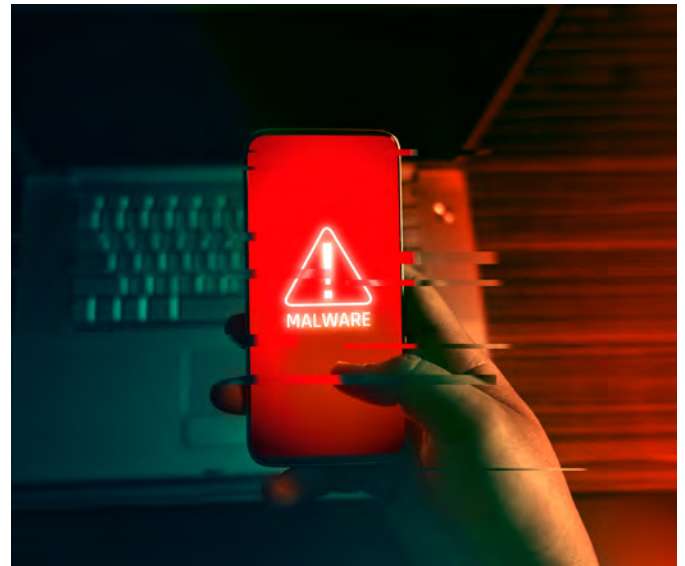
Mobile Biometrics Face Privacy Risks And Vulnerabilities

If a password is stolen or compromised, the user can simply change it. But the same user cannot change a compromised fingerprint or iris. Even if users' fingerprints aren't compromised, biometric thievery can take other forms.

If a malicious actor lifts a clear impression of a user's fingerprints from a glass, a doorknob or even a phone, the hacker would be able to create a prosthetic fingerprint that he or she could then use to spoof the device's sensor.

Cybercriminals could possibly piece together a credible facial image that could fool a mobile device, perhaps using photos freely available through social media or other sources. Executives and other users with access to critical financial information and trade secrets may be worthwhile targets for these resource-intensive attacks.

Mobile devices that rely on fingerprint authentication might also be at risk from hacking attempts that use master fingerprints. Researchers have demonstrated that they can generate master fingerprints from numerous sample prints and use those master prints to access different devices. Spoofing and hacking aren't the only challenges that come with biometric authentication for mobile devices. Biometric technologies rely on immutable physical features that will



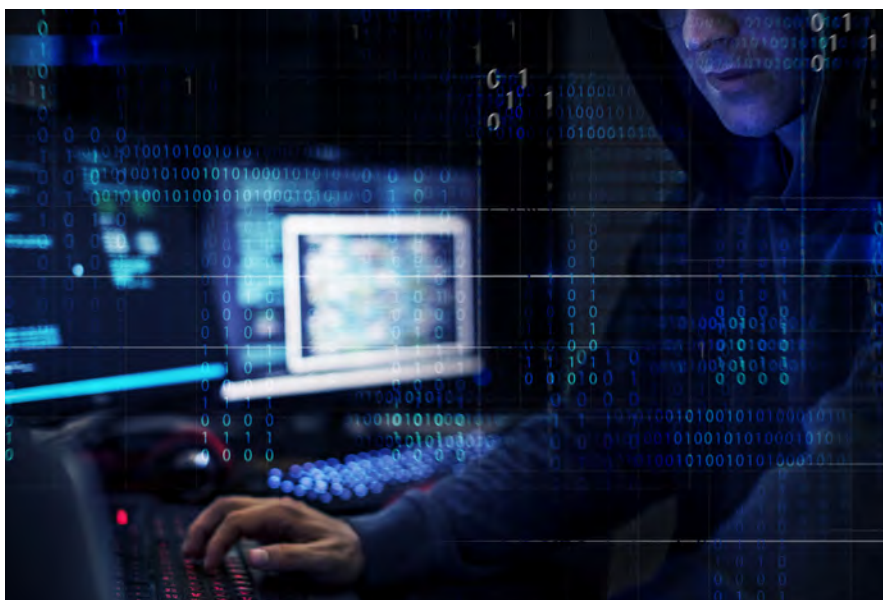
not change for as long as they're needed. However, injuries, illnesses, weight loss, plastic surgery or other events that change physical characteristics can potentially disrupt the authentication process, making it more difficult for users to access their own devices. Even a paper cut on a user's finger could be enough to deny him or her access to a mobile device.

Legal Challenges To Biometrics

Both Android and iOS devices go a long way in protecting biometric data, and some experts believe the benefits of mobile biometrics far outweigh the risks. Some users may still be reluctant to trust those devices with their biometric data, which could create a tricky situation for organisations that want to employ biometric authentication for mobile devices.

Forcing employees to use biometric authentication might raise privacy and legal concerns. In fact, there is already litigation around forced biometrics in the enterprise. The focus of current legal concerns is related to other forms of biometrics, such as employee time clocks, but these issues could easily spill over to mobile devices.

The trajectory of enterprise mobility is moving at lightning speed toward a greater reliance on biometrics. And until a better alternative comes along, that's not likely to change anytime soon. Organisations will have to anticipate user pushback and biometric attack vectors to ensure effective mobility management.



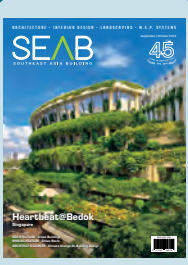


Subscription Form

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

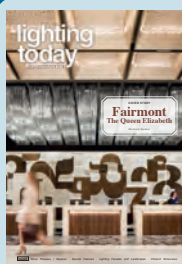


SINCE 1994

☐ 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

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: _____



Dahua Technology Singapore +65 6538 0952 sales.sg@dahuatech.com www.dahuasecurity.com IFC



Microengine Technology Malaysia +603 7957 2008 enquiry@microengine.net www.microengine.net 5
 Delta Scientific U.S.A. +1 661 575 1100 info@DeltaScientific.com deltascentific.com 3



Avigilon U.S.A. +1 888 281 5182 asksales@avigilon.com www.avigilon.com 7
 Johnson Controls Singapore +65 6319 9820 bts-apac-detection-products@jci.com www.zettlerfire.com 9

See us at following upcoming events!

Event	Date	City	Country	Website	Page
Safety & Security Asia 2019	1 - 3 Oct 2019	Singapore	Singapore	www.safetysecurityasia.com.sg	1
ISC West 2020	18 - 20 Mar 2020	Las Vegas	U.S.A.	www.iscwest.com	IBC
Secutech India 2020	7 - 9 May 2020	Mumbai	India	www.secutechexpo.com	15
IFSEC International 2020	19 - 21 May 2020	London	United Kingdom	www.ifsec.events/international/	OBC
IFSEC SEA 2020	23 - 25 Jun 2020	Kuala Lumpur	Malaysia	www.ifsec.events/kl/	11
IFSEC Philippines 2020	22 - 24 July 2020	Manila	Philippines	www.ifsec.events/philippines/	13



PREMIER SPONSOR:



CONNECTED
SECURITY

DRONES &
ROBOTICS

EMERGING
TECH

LOSS PREVENTION
& SUPPLY CHAIN

PUBLIC
SAFETY

SMART
HOME

SAVE THE DATE



COMPREHENSIVE SECURITY FOR A SAFER, CONNECTED WORLD

- Discover the industry's latest products, technologies & solutions
- Network with 30,000+ Physical, IoT and IT Security Professionals
- Direct access to 1,000 leading exhibitors & brands
- 85+ SIA Education@ISC Sessions



SIA EDUCATION@ISC:
MARCH 17-19, 2020

EXHIBIT HALL:

MARCH 18-20, 2020

SANDS EXPO, LAS VEGAS

Register today at:

ISCWEST2020.COM/TLM

#ISCWEST

IFSEC

INTERNATIONAL



SAVE THE DATE

IFSEC International returns
19-21 May 2020, ExCeL London

Co-located with:

FIREX
INTERNATIONAL

**SAFETY &
HEALTH** EXPO

**FACILITIES
SHOW**

Plus:

