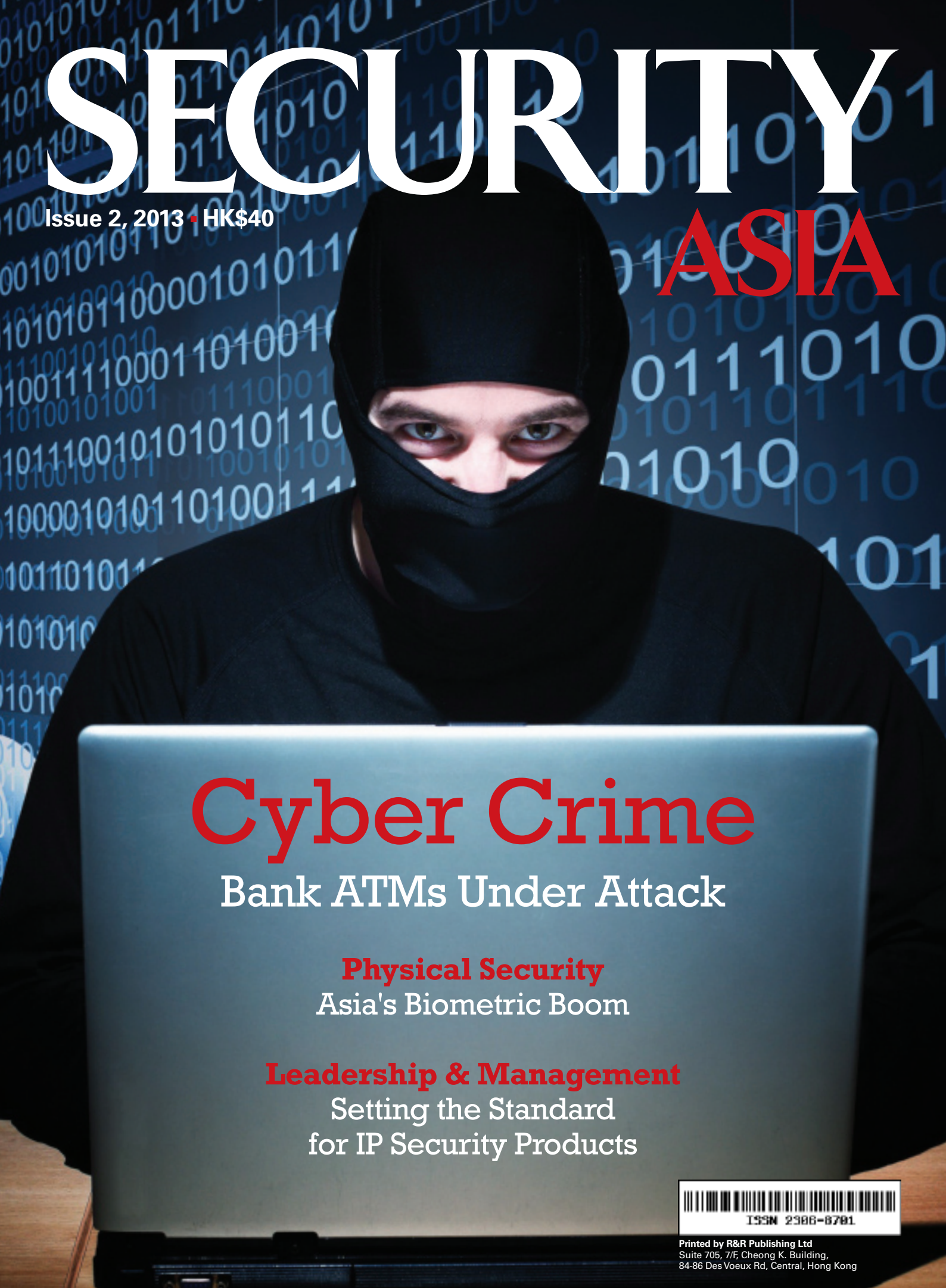
SECURITY ASIA

Issue 2, 2013 • HK$40



Cyber Crime

Bank ATMs Under Attack

Physical Security
Asia's Biometric Boom

Leadership & Management
Setting the Standard
for IP Security Products

ISSN 2306-8701

Printed by R&R Publishing Ltd
Suite 705, 7/F, Cheong K. Building,
84-86 Des Voeux Rd, Central, Hong Kong

SECURITAS

A Knowledge Leader in Security
保安業智慧領航者

Specialized Guarding 專門護衛
Gurkha Officers 喼喀保安
Technology Solutions 保安科技方案
Mobile Patrol 巡邏服務
Key-Holding and Alarm Response 持匙服務及警鐘監控
Event Security 大型活動保安
VIP Protection 貼身護衛
Consulting and Investigation 保安顧問及調查服務

Phone: +852 21918918 **Email: info@securitas.hk**

www.securitas.hk

Publisher
Richard Silkstone, R&R Publishing Ltd

Contributors
Stuart Sanders, Velocity Solutions;
Jill Wong, Trefor Moss; Jill Wong, Isabella Wong and Johanna Yau, King & Wood Mallesons;
Claudio Scarabello, Verizon Enterprise Solutions

Staff Writer
Colin Robson

Publication Manager
Ian Harling
T: (+852) 2126 7815
E: Ian@RRPublishing.com.hk

Advertising Sales – Print & Web
Colin Robson
T: (+852) 2126 7812
E: Advertising@RRPublishing.com.hk

Regional Advertising Representative
EBconcepts
Edo Bersma
T: (+852) 9641 1936
E: Edo@EBconceptsHK.com

Circulation
Ian Harling
T: (+852) 2126 7815
E: Circulation@RRPublishing.com.hk

Web Manager & Design
Ian Harling

Magazine Design
Jacky Ngan

www.Security-Asia.net

Endorsed by:
The Hong Kong Security Association

Circulation of Security Asia
Over 4,000 copies delivered directly to the following associations and decision makers who are responsible for the purchasing of security related services and products:

- Members of HKSA
- Government security bureaus
- Security consultants
- Law and accountancy firms
- Financial institutions
- Insurance companies
- Facilities management providers
- Security hardware and software manufacturers

Also available at:
- Security exhibitions
- Conferences and seminars
- Quality book stores

Published by R&R Publishing
Suite 705, 7th Floor
K. Cheong Building
84-86 Des Voeux Road Central
Hong Kong, SAR
Tel: (+852) 2126 7815
Info@RRPublishing.com.hk

www.RRPublishing.com.hk

ISSN 2306-8701

CONTENTS

香港保安業協會
HONG KONG SECURITY ASSOCIATION

THE HONG KONG SECURITY ASSOCIATION

The Hong Kong Security Association and our members are dedicated to provide and maintain the best service and product standards.

The Hong Kong Security Association was founded in 1984 and is the only Association of companies holding security licenses issued by the Security and Guarding Services Industry Authority.

Our member companies are principally engaged in providing many different apects of security services:

- **Guarding services-commercial and residential.**
- **Cash transport services by armoured vehicle.**
- **Installation and maintenance of alarm systems and equipment.**
- **Remote monitoring of alarms, fire alarm and CCTV systems.**
- **Supply of security systems and products.**
- **Investigation and security consultancy services.**

The Association works with the Security & Guarding Services Industry Authority for the regulation of the industry.

The Association works closely with the Security Companies Inspection Unit of the Crime Prevention Bureau of the Hong Kong Police Force.

The Association, being a member of the Security Services Training Board of the Vocational Training Council contributes towards quality framework and training standards.

The Association forms working groups to tackle assignments and special projects.

The Association holds social functions to provide platforms for idea sharing and opportunity for members to meet.

We are here to support you and the Industry.

Become a member of the Hong Kong Security Association today.

HK SECURITY ASSOCIATION
T: 2960 1142
F: 2960 4262
E: thehksa@netvigator.com
W: www.thehksa.com

Security manpower shortage looms in Hong Kong

MESSAGE FROM THE HKSA CHAIRMAN

By Douglas Renwick

The Hong Kong security industry is facing a critical manpower shortage affecting all aspects of the security industry: from guarding to system installation and armoured vehicle services. With low unemployment rates and rising demand from increasing numbers of commercial and residential buildings requiring security services, best estimates are the industry is facing a 10-12% manpower shortage. This translates to an additional 10,000 people.

Many potential staff have been attracted to other industries such as hotels and the retail sector; others have transferred to the construction industry led by an increase in government funded construction projects and government sponsored training and retraining programmes to attract potential employees.

Without the ability to import labour to cover these manpower shortages the security industry and end users of security services will suffer. These issues - if not quickly addressed - could lead to a potential rise in crime rates and security related issues; perhaps in future we may see the government increasing the size of the police force to combat the rise in crime!

The Chief Secretary released a document to the Legislative Council House Committee back in March 2013 stating the committee's intention to study the importation of semi-skilled workers. As the Hong Kong workforce is forecast to shrink after 2018, is this too little, too late?

The industry is looking internally at all the options available to attract new recruits; salary is not the only driver – often younger people prefer working fewer hours per day or less days per week. On average most people in the industry work 12 hours per day and 6 days a week. When you add in travelling time this is indeed a long working week and certainly a factor that needs to be addressed.

Reducing working hours or moving to a 5-day week also has its issues. Reducing working hours from 12 hours to 9 hours per day creates a need to recruit additional people

to meet customer requirements for 24 hour coverage. Where are these additional people to be recruited from? Moreover, in reducing working hours or days per week, we should not see a reduction in take-home pay otherwise it becomes self-defeating. The time has come for end users of security services to accept the fact that the costs for security services will rise. Service providers need to remain steadfast and maintain charge rates, especially at a time when the shortage of labour is significant. It may even be time for them to consider increasing charge rates to ensure they have sufficient funding to increase staff salaries, shorten working hours, invest in staff training and develop and retain employees.

Additional short term measures could help ease the burden created by a lack of manpower, such as changing definitions set out under the Security Personnel Permit (SPP). Currently, employees over the age of 65 can no longer work in 95% of the buildings and facilities in Hong Kong as they have to change their security permit from Category 'B' to Category 'A'. This means they can only work at strictly defined locations, namely 'single private residential buildings'. A permanent or temporary relaxation of this definition could, for example, cover normal residential buildings, commercial buildings or even open car parks, all of which are restricted at present. This could help employers retain their staff for longer periods, thus reducing manpower shortages.

Although some employees may not wish to work over the age of 60 or 65, many staff do want to work but are restricted under the current licensing ordinance. This is especially interesting when all reports suggest that people are now living longer, are healthier, fitter and remain capable and active in old age. Enacting small changes to the current licensing requirements would require policy change and a political willingness to ensure that healthy, fit and willing staff over the age of 65 (numbering 0.98 million in 2012 and rising to 2.56 million in 2041) can continue to work in the industry. Their experience, knowledge and dedication should be acknowledged and appreciated. ■

BANK ROBBERY

v.2.0

Cyber-criminals are now capable of stealing more from banks than old-fashioned bank robbers ever could. So as cyber-attacks grow more sophisticated and ambitious, are financial institutions losing the battle to keep our money safe?

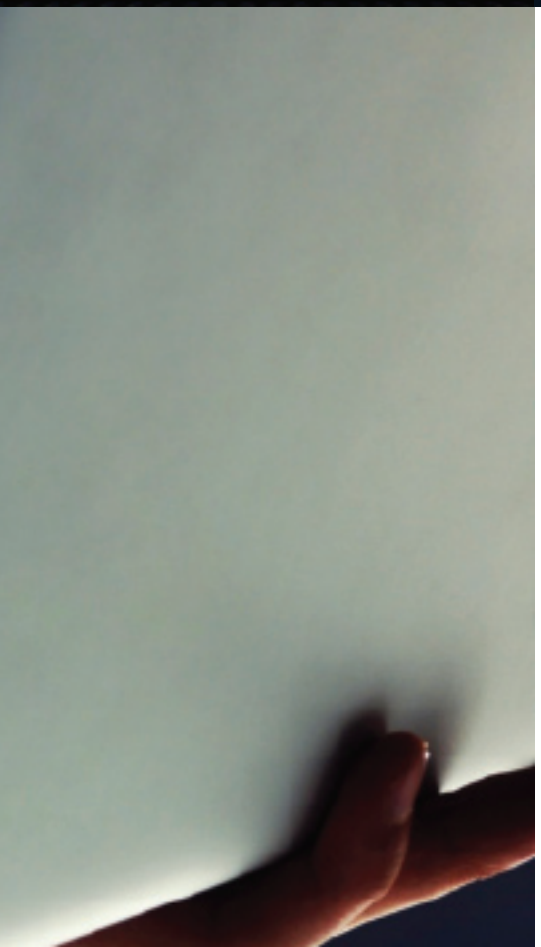
Information technology has revolutionised the way society handles money – and that includes the way in which we steal it. This was never more apparent than on one day in late February, when a criminal syndicate took the cyber-heist to an entirely new level.

Within the space of just a few hours, gangs of thieves operating across 26 countries withdrew $45 million from hundreds of ATM machines. But they were only foot-soldiers in a complex form of cyber-attack known as an "unlimited operation" – unlimited in the sense that there is no ceiling on the amount of money that can potentially be stolen.

The brains behind the operation – who, unlike many of the thieves on the ground, have not yet been traced – were sophisticated hackers who had succeeded in penetrating the systems of two credit card processing companies based in India and the US. This in turn enabled them to steal all the necessary information relating to 17 accounts held with two banks, one based in Oman and the other in the UAE, and also to remove any ATM withdrawal limits associated with those accounts. Finally, armed with this data, their operatives on the ground were able to clone the account holders' credit or debit cards; they then withdrew as much cash as possible before the financial institutions involved realised what was happening and were able to block further withdrawals.

This was not the first "unlimited operation" to have succeeded in harvesting millions from ATM machines: in 2012, $9 million was stolen within the space of two hours from ATMs across Europe in a similar heist, according to internet security firm Symantec. However, the February 2013 attack was the most audacious undertaken so far, and it has set alarm bells ringing across the globe about the ability of our financial institutions to withstand well resourced and highly co-ordinated cyber-attacks.

"With the world of banking – an early adopter of IT solutions – moving to the digital world for convenience and transparency, criminals have realized that the cyber route to a bank heist is as profitable and even easier [than traditional robbery]," explains Lawrence Li, systems engineering manager, Symantec Hong Kong. And while the recent heist grabbed headlines by virtue of the sums involved, Li says the problem is older and rooted more deeply than many



people realise. "Cybercriminals have been defrauding financial institutions and their customers of millions of dollars annually," he says.

There also appears to be little question that the $45 million heist was the work of technically accomplished criminals. "I would say that the front end of the operation was quite sophisticated and required identifying the payment processor and looking for vulnerabilities in web-facing applications in order to the exploit the infrastructure and gain entry to the account data," explains Marty Meyer, president of Corero Network Security, a US-based provider of online security solutions. Li adds that the hackers would have needed detailed knowledge of the banks' infrastructure, and would have "created very targeted malware" with which to perpetrate the attack.

Meyer points to the fact that the hackers identified a weakness in the banks' defences – not necessarily in the banks' own systems, but in those of the third-party companies they employed to process their customers' payments. Financial institutions, including household names like Visa and Mastercard, commonly outsource payment-processing functions to IT firms which specialise in this particular banking-technology niche. However, according to Meyer, this practice can create weak links in the bank's data security arrangements. "If they follow PCI regulations, they should not be a weak link, but [the payments processors involved here] may not have complied fully with these types of regulations."

Financial institutions around the world have adopted a series of Payment Card Industry (PCI) standards to ensure that payments are processed securely. For this reason, "banks are the gold standard when it comes to cyber-security," argues Doug Johnson, vice president of risk management policy at the American Bankers Association, with security systems used by the industry "sophisticated and constantly evolving to anticipate potential threats". As a result, there were only 18 data breaches recorded across the US financial sector in 2012, according to Johnson, citing statistics from the Identity Theft Resource Centre – far fewer than in other sectors, including business (173 breaches) and medical/healthcare (163).

Meyer suggests that some institutions, even if they pay sufficient attention to their own security systems, are not doing necessarily enough to scrutinise the security arrangements of their third-party contractors.

Outsourcing Risk

However, Meyer suggests that some institutions, even if they pay sufficient attention to their own security systems, are not doing necessarily enough to scrutinise the security arrangements of their third-party contractors. "In most cases it should be quite difficult [to hack into a payment system] assuming all PCI standards have been met," he explains. But he adds that "smaller regional banks and credit unions who often outsource their online banking operations" need to send risk and compliance teams "to perform proper diligence on any third-party service provider to make sure that protection against modern cyber-

threats is in place".

Unfortunately, the sheer scale of the global financial services industry makes the banks a huge and porous target for any organised criminals with the patience to study the system internationally until they find a weakness they can exploit. For governments and for the banks themselves, the extraordinary success of the recent cyber-heist is a particular worry given the fact that the finance industry is already subject to relatively tight regulations when it comes to cyber-security. Most private companies are under no obligation to invest in cyber-security systems, though many are now choosing to do so as the cyber threat level steadily escalates. But banks, given the extremely sensitive and valuable nature of the data which they hold, are meant to adhere to the PCI standards and take various measures to test the robustness of their networks. The heist's success exposed the fact that some within the industry are failing to meet those standards.

A spokesman for Mastercard told Security Asia that the company's own systems had at no point been compromised during the heist, citing the "comprehensive fraud management program" which it has in place. Instead, he laid the blame for the security breach squarely at the door of the two third-party processors – Indian firm EnStage, and ECS, its US counterpart – by pointing out that "both companies have been delisted as PCI DSS [Data Security Standard] compliant" in the wake of the February robberies.

The challenge is that cyber-crime is evolving so quickly that security systems which companies operate may become outdated much sooner than they realise. "Relying on traditional technology, such as firewalls and intrusion prevention that was developed ten plus years ago is not a strategy that will protect an organization against untrusted and unwanted network traffic," warns Meyer.

Most cyber-attacks against banks are not as intricate as the February heist, of course. An increasingly common form of attack is the Distributed Denial of Service (DDoS), a tactic which involves bombarding a website with huge volumes of traffic, thus crowding out genuine users. It can have a variety of objectives. Some hackers may not have theft in mind when they launch a DDoS against a bank – these institutions lose money if their customers cannot bank online, and this kind of disruption may be the only objective. But often robbery is the ultimate goal. "Sensitive data is not directly at risk from DDoS attacks," explains Meyer, "but such attacks are typically used to distract bank IT staff and bank customers from other attack vectors launched simultaneously that can inject Trojans or malware or other remote executable code into the bank network which can then be used to extract this data."

A Trojan is a piece of software which appears benign, but which has a hidden, malicious purpose, and according to Symantec these programs are causing particular problems for financial institutions. "Today's attackers are using a new trick in the book – the banking Trojan,"

says Li, "and these threats are affecting financial institutions around the globe; over 600 have been targeted already.

"These financial Trojans install on a user's computer and specifically target user accounts of many financial institutions," he continues. "Banking Trojans enter through the backdoor, strike with clinical precision, and have evolved to a degree of sophistication that allows attackers to conduct high-value transactions while evading traditional fraud-detection measures. The attackers behind these Trojans are organised underground groups who are not only experts at scripting and automating attacks, but also understand the sophisticated global financial industry." The big challenge which banks face when meeting this type of threat, Li explains, is that most existing security systems "are ineffective at protecting against the modern banking Trojan", since they are more geared towards detecting older kinds of cyber-threat, such as viruses.

Arguably the most sinister aspect of the Trojan phenomenon is that Trojans are available as off-the-shelf products, and can be obtained for just a few hundred dollars for a basic version, or up to several thousand dollars for an advanced program. This bank-robbing software is the product of an increasingly organised criminal fraternity, according to Li. "The underground financial fraud community has become increasingly organised," he explains. "Everything from bots and intelligent configurations to localised distribution channels are being bought and sold. Attackers are no longer just participating in financial fraud; some are dedicated to tool creation to facilitate these activities. The underground community is a service industry."

New Tactics

One of the financial Trojans produced by this burgeoning industry is a program called Citadel, which first emerged in 2011. It has since infected computer systems around the world, with 75 percent of all instances discovered in just three countries: Australia, Italy and the US. It operates by installing malware onto targeted computers and turning them into 'bots', or elements of a 'botnet' – a network of computers brought under the criminals' control to perform whatever functions they require.

In June 2013 Microsoft announced that it had been working with the financial services industry and the FBI to take down over 1,000 Citadel botnets, thus seriously disrupting, if not entirely eradicating, the Citadel threat. However, despite this moment of success, this kind of attack against financial institutions is becoming increasingly commonplace. Symantec's Li observes that "web-based attacks increased by 30 percent in 2012", and points to another popular new tactic, known as a "watering hole" attack. "In a watering hole attack, the attacker compromises a website, such as a blog or small business website, which is known to be frequently visited by the victim of interest," Li explains. "When the victim later visits the compromised website, a targeted attack payload is silently installed on their computer." This offers attackers another potential weak point – rather than attack the well-protected bank itself, the criminals identify a small business with which the bank interacts as a potential watering hole, and then compromise it with malware.

Another potential vulnerability which hackers use to bypass the banks' defences is the "endpoint", devices such as phones and laptops which bank employees commonly use – but which the institutions themselves often fail to secure to the same degree as their in-house systems. The BYOD trend – "bring your own device" – is the Achilles heel of many cyber-security systems, with companies unwittingly sacrificing security in order to boost productivity and convenience.

With so many potential points of weakness, and so many new and evolving tools in the hacker's toolkit, it is perhaps surprising that a heist on the scale of the February event does not happen more often. Johnson of the ABA points to the tough security standards which most banks adhere to, and also to information-sharing mechanisms, such as the Financial Services Information Sharing and Analysis Center, which enables financial institutions to pool knowledge about the existing threats.

However, Symantec considers the cyber-threat level to be rising fast. "Attacks that can intelligently target large numbers of institutions concurrently will intensify," says Li. "Sophisticated

cybercriminal groups are already using advanced techniques like automated transaction services (ATS) and traffic direction services (TDS). These are services that the underground service community is streamlining." ATS is the evolution of cruder cyber-crime programs which previously attempted to steal bank account details, for example, by displaying a pop-up which, posing as an element of the bank's own website, asked users to input their information. But ATS is more subtle: it runs unseen, and harvests account information when the user banks online, even making illegitimate transactions which the user cannot detect. TDS, meanwhile, is a sophisticated means of diverting web traffic towards a malicious site where the user unwittingly becomes exposed to malware.

Yet despite the growing complexity of these threats, most financial institutions should be able to remain secure most of the time. "While it is not likely that you can always stay one step ahead of every attacker and prevent 100 percent of attacks, you can make reasonable investments to prevent the risks posed by a large majority of the attacks that exist globally," concludes Meyer. Banks need to accept that highly motivated and well organised criminals are targeting their networks, and properly resource their countermeasures, he says. "This is the new normal, and banks need to take a layered security approach to cast the widest net to prevent these attacks and the risks they pose."

According to Li, financial institutions with concerns about their network security should focus on the potentially extreme cost of a security breach, rather than on the relatively small cost of upgrading their equipment. "Computers and servers can be replaced relatively simply," he argues. "It's far more costly to notify thousands of customers that their information was compromised and deal with the resulting loss of their trust and business, not to mention the financial penalties." He also counsels that "one size does not fit all" when it comes to cyber-security systems – banks need to work with a cyber-security systems provider and develop a solution tailored to the size of their organisation and the type of data they want to protect. They also need to extend that security to any mobile devices which connect with the company network, and train their employees thoroughly in network security best practice.

There will undoubtedly be more spectacular heists like the $45 million event of February 2013. So many criminals armed with so many sophisticated pieces of software are bound to find the occasional flaw in the security architecture of the global banking system, and exploit it to dramatic effect. However, by securing their own networks – and exhaustively vetting the systems of the companies they interact with – banks can ensure, within reason, that they will not be the next ones in the limelight when the cyber-thieves strike. ■

Another potential vulnerability which hackers use to bypass the banks' defences is the "endpoint", devices such as phones and laptops which bank employees commonly use – but which the institutions themselves often fail to secure to the same degree as their in-house systems.

Setting the Standards

Security Asia **recently had the opportunity to talk to Mr Per Björkdahl, the Chairman of ONVIF's Steering Committee since November 2012. ONVIF is an open-industry forum created to develop and promote global standards for the interfaces of IP based physical security products. Per is also Director of Business Development for Axis Communications, one of the three founder members of ONVIF.**

Q: Per, briefly tell us how you became involved in technical convergence.

I've worked in the technology field all my professional life. Before joining Axis I worked in the automation industry and when the internet took off around 1995, bringing with it the capability to transmit large amounts of information long distances in a standardised way, I saw convergence really coming into its own. If you think of convergence as two technologies coming together to form a third, then the rise of the internet brought about the possibilities of convergence.

Q: You were recently rated No. 3 in IFSECglobal.com's Top 40 Most Influential People. How do you feel about that?

Firstly, I was a bit surprised – I didn't realise that by representing an organisation such as ONVIF I would be a candidate. IFSEC is a highly respected organisation globally and if they recognise that a standardisation organisation such as ONVIF has that much influence in the industry, I feel encouraged by that recognition.

Q: Are people becoming more aware of ONVIF's work in light of this accolade?

ONVIF is now more focused on reaching out to the public. For example, at IFSEC this year we had our own booth and

we invited around 15 manufacturers to demonstrate interoperability. We also gave presentations on certain days. Events such as these help raise our profile.

Q: ONVIF has been in existence for 5 years now. Please describe how the organisation came into being and the initial aims.

In most converging industries there is a drive to eliminate some of the development hurdles to allow a technology to really take off. The three manufacturers that started ONVIF, Sony, Axis and Bosch, represent a large portion of the security camera market and initially membership was only open to manufacturers of network video products. The original three companies identified the need for interoperability and a standard to drive the technology forward and now ONVIF is open to any IP based security device manufacturer.

Q: Did you find some CCTV manufacturers initially resistant to the idea of interoperability and more focused on proprietary systems?

From a manufacturing point of view, and certainly from the viewpoint of the top three brands, we want to fuel more activity in the market. One of the ways we can do this is by eliminating obstacles to the development of the technology and one of the clear obstacles when it comes to product development is interoperability - or rather the lack of it. If a system developer has a cool idea for a new camera feature, where does he concentrate his efforts? Does he spend a great deal of time developing drivers for all the leading brands and have few resources left over for the application – or does he fully develop his application and then choose manufacturers to work with? This is where interoperability benefits innovation; you spend far less time integrating hundreds of brands and focus your energy on the application.

Manufacturers also have little to gain by being held to ransom by a VMS manufacturer who tells the end user: you can only choose between the cameras on this list because these are the cameras I support. That's not helpful, especially if you're not on the list!

Q: So the drive for standardisation won't stifle innovation?

No. Let's take Power over Ethernet (PoE) as an example. PoE has been around for many years and initially Cisco and PowerDsine each promoted their own PoE implementation. However, it wasn't until the IEEE became involved and a standard agreed that the number of PoE devices on the market rose sharply.

What really defines a standard, especially a de facto standard, is when it earns its dominance through free will and people's choice. Once dominance is achieved, the manufacturers, the users and the supporting community realise this is the way to go forward.

Q: ONVIF released Profile S in Jan 2012 and Profiles C and G are due for release later this year. What is the concept behind ONVIF's profile specifications?

In the beginning, ONVIF created a specification which contained a very large number of functions. Very few of these functions were mandatory and as a result, different manufacturers developed different sets of features. Their products were conformant but not interoperable because of the different features. They spoke the same language, so they could ask for things, but they may not have got what they asked for – if you see what I mean. The introduction of profiles allows us to set a limited number of features as mandatory requirements. For example, Profile S mandatory features include device discovery, pan/tilt/zoom and audio, and products must support these features to be Profile S compliant. This means we have Profile S conformant VMS and Profile S conformant products; they agree on the same functions so there is no mismatch in communications.

The introduction of profiles allows us to set a limited number of features as mandatory requirements. For example, Profile S mandatory features include device discovery, pan/tilt/zoom and audio.

Profile G addresses video storage – storing, retrieval and playback and Profile C incorporates the basic features of an access control system. Profile S is currently available and manufacturers can prove their products are Profile S conformant. Profiles G and C are release candidates; that means the documentation has been made public on our website, although it remains in release candidate format. The official release is planned for the end of the year.

Q: As devices offer more features and functions, does ONVIF automatically update its specifications to accommodate developments?

It takes the consensus of three full members to propose a new profile.

ONVIP steering Committee Chairman Mr. Per Björkdahl

Considering the Profile S base, I would say maybe 85% of all manufacturers' camera functions are covered. There will always be special functions that distinguish, say, an Axis camera from a Bosch camera, and I think that's necessary as it has to be more than just the colour of the product that differentiates it in the marketplace. Manufacturers still have the legroom to develop unique features.

Q: How many manufacturers are now making products to ONVIF specifications?

Last week we had 449 member companies so by now I'm pretty confident that number has risen above 450.

Q: How are you going about educating the public and end users regarding ONVIF benefits and profiles?

We do a lot of press interviews and I've set out on a mission to speak to security associations and related bodies to explain what ONVIF is about and what you can expect. I think it's easy to create a false impression - especially in very fast-moving technology. For example, some people may expect full interoperability, which is a very big task to achieve.

Q: PSIA (Physical Security Interoperability Alliance) began at the same time as ONVIF and initially was hailed as easier to use by many end users. Is it fair to compare ONVIF and PSIA to the VHS/Betamax outcome?

I honestly don't know. Several of our members are also members of PSIA. We work very hard for the same purpose and try to the best of our abilities to attract members and products. We both do the same thing but we do it slightly differently technology-wise. I believe in what we do and I stand by that.

Q: What is the next milestone for ONVIF?

The next milestone will be the public release of Profile candidates G and C by the end of this year. We have an annual meeting in Shenzhen in October where we'll be creating momentum for the new profiles and looking at what features the industry wants standardised.

Q: Do you see applications for ONVIF outside the security industry?

Not outside the security industry. The scope of ONVIF is to provide interoperability for IP based physical security products. I'd say the next step will be the provision of something within the security industry, for example: intrusion alarms, maybe additional S profiles, additional C profiles.

Q: When do you think we'll see ONVIF adopted as a standard rather than a specification?

If the definition of becoming a standard is recognition by an official standards body, we have just passed that mark. The international standards body, the IEC, has been working for some time on IEC 62676-2, and this standard adopts a complete ONVIF specification. Future IEC work will also be based on complete ONVIF specs. Now that there is a standard – and a lot of effort has been put into it – I think we'll see government projects and suchlike specifying compliance. ONVIF is a de facto standards group and it will remain so - that's the purpose of it. When you work with standards you put in a lot of effort, and if you can harmonise with what's happening in the industry, I think that's a good thing. ■

If the definition of becoming a standard is recognition by an official standards body, we have just passed that mark. The IEC has been working for some time on IEC 62676-2, and this standard adopts a complete ONVIF specification.

And your #1 choice for quality, innovation and expertise.

- The founder of the world's first network camera
- The world leader in network video, driving the shift from analog to digital
- Sweden-based company, with over 16 years of experience in IP video and nearly three decades of network know-how
- Installations worldwide in sectors ranging from retail and transportation to education and city surveillance
- Dedicated partner network offering unrivaled expertise
- Solutions delivering enduring results, even in the most extreme conditions and remote locations
- Open standards only, for easy integration and scalability

Get the Axis picture. Stay one step ahead.
Visit www.axis.com

ONVIF
Driving IP-based physical security through global standardization

AXIS COMMUNICATIONS

Safeguards Against Money Laundering

In this article, we discuss the hot topic of money laundering and how robust security systems and internal policies and controls can safeguard you and your company against this risk and exposure to liability under Hong Kong's increasingly strict anti-money laundering (AML) laws.

Hong Kong's legal landscape

Hong Kong is an international financial centre and aims to comply with international standards to combat money laundering. In April 2012, Hong Kong created a new weapon with which to wage this war, that is, the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap. 615) (AMLO) came into effect.

Before April 2012, Hong Kong mainly relied on the following ordinances to combat money-laundering and terrorist financing:

- Drug Trafficking (Recovery of Proceeds) Ordinance (Cap. 405)
- Organized and Serious Crimes Ordinance (Cap. 455)
- United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575)

Money laundering includes a wide range of activities or processes which changes the identity of illegally obtained money (that is, the proceeds of crime) to disguise its illegal origin, whilst terrorist financing can be simply described as financially supporting terrorist acts and terrorist organisations. The AMLO runs parallel with existing laws to combat money laundering and governs financial

institutions, such as banks, brokers, insurance companies and money service operators.

Key things to note about AML laws

Any person may be held liable for:

- dealing with property representing proceeds of drug trafficking or other indictable offences (for example, tax evasion and money laundering)
- providing or collecting funds for a terrorist act (that is, terrorist financing)
- failing to report knowledge or suspicion of money laundering or terrorist property
- tipping off
- prejudicing investigations

In respect of financial institutions, AMLO further:

- mandates customer due diligence and record keeping as compulsory requirements for financial institutions; and
- enpowers the relevant authorities to conduct investigations and take disciplinary action.

Long sentences are becoming the norm for money launderers, and huge fines are imposed on the institutions that "turn a blind eye" or who have gaps in their systems and controls that allow money launderers to carry on their criminal activities. In Hong Kong, two recent cases involving a young delivery man and a public housing tenant, both of whom were convicted of money laundering several billion Hong Kong dollars, were sentenced to 10 years in prison. Overseas, a well-known bank was fined US$1.9 billion for various AML violations.

What safeguards should you think about?

(1) Build a monitoring and reporting system for suspicious transactions

Any person who comes across any property (including money) which he knows or has reasonable grounds to believe is the proceeds of drug trafficking or of an indictable offence, or is terrorist property, is obliged by law to make a suspicious transaction report to the Joint Financial Intelligence Unit (JFIU), a joint body comprising staff from the Hong Kong Police and Customs & Excise Department, as soon as practicable. Having a system or procedures in place to help you identify potential crimes and suspicious transactions will help you with this requirement. For many institutions, the use of an IT system designed with specific parameters to identify suspicious transactions is a good solution.

For financial institutions, good AML systems and controls are vital. The AMLO has criminal penalties that apply to individuals (as well as the institution) so if you are an employee of a financial institution and you knowingly cause or knowingly permit your institution to contravene the AMLO, you could be liable to a fine up to HK$1 million and imprisonment for 2 years. However, there is a defence if you acted in accordance with the AML policies and procedures of your employing institution; hence underlining the importance of good internal controls.

(2) Have good record keeping

Maintaining proper records is fundamental to any business. Records of customers' identities and corporate documents and of transactions with or through you, for example, mean that you can support an explanation that you had no knowledge or belief that you were dealing with the proceeds of crime.

(3) Awareness training

Money laundering is not just an issue for financial institutions; the AML laws (other than the AMLO which applies specifically to financial institutions) apply to everyone. Ignorance of the law is no excuse. What if you provide security services for a VIP whom you know or have reasonable grounds to believe is a drug dealer and large amounts of cash was used to pay for your fees? By accepting payment for your services, you may be exposed to allegations that you have dealt with the proceeds of crime. In order to keep on the right side of the law, you should lodge a suspicious transaction report with the JFIU. Knowing the right steps to take will protect you and your organisation. ■

Money laundering is not just an issue for financial institutions; the AML laws (other than the AMLO which applies specifically to financial institutions) apply to everyone. Ignorance of the law is no excuse.

JILL WONG, ISABELLA WONG AND JOHANNA YAU; KING & WOOD MALLESONS

This article is only a general outline. It is not legal advice. You should seek professional advice before taking any action based on its contents.

Asia's Biometric Boom

We are all physically unique – and having the ability to recognise an individual's unique attributes and then making use of that valuable information is what biometrics is all about.

For Asian governments this kind of capability is priceless. They are under pressure to secure their borders, both to guard against terrorist threats and to manage ever greater inflows and outflows of people. Meanwhile, the demands of managing a complex modern economy require them to have a clearer picture of who and where their citizens are, whether the objective is to control internal migration, or to be sure of providing the right social services, or even the right salaries, to the right end users. Private companies are also more and more interested in having an effective means of identifying their employees in order to secure their businesses and transactions.

Biometric technology in its various forms is able to help public and private concerns to meet these changing needs. The global market for biometric systems will grow to $20 billion by 2018, according to a recent study by TechSci Research; and while Europe and North America account for 60 percent of the market today, demand for biometric technology is rising quickly in Asia.

The citizens of some Asian territories are already familiar with biometric border-control systems: Hong Kong residents, for example, carry biometric identity cards and have their thumbprint scanned whenever they cross the border. Malaysians have been familiar with the technology for even longer: their country was the first in the world to introduce biometric passports in 1998. However, national biometric schemes in China and India are now bringing about the adoption of this technology on an unprecedented scale.

The different technological paths available when creating a biometric system ultimately amount to the same thing: the ability to identify with near-certainty the identity of an individual. In addition to fingerprint recognition, iris scanning, facial scanning, voice recognition and hand-vein recognition are the main approaches to recording the unique features of individual citizens. But each system is best suited to a particular application. "Face recognition is the most suitable technology when you want to recognise an individual covertly [such as via CCTV surveillance]," explains Liu Xiaoming, a professor at Michigan State University's Department of Computer Science and Engineering, which specialises in biometric research. In contrast, "when a user is fully cooperative, iris recognition is the most accurate modality," he says.

In order to improve accuracy, India's Universal ID (UID) programme incorporates three of these systems: when fingerprint recognition alone was found to be insufficiently accurate, the government added facial and iris scanning to its ID card plans. However, the challenges involved in building up a biometric database of 1.25 billion people are hard to understate – indeed, the minister in charge of the scheme has summed it up as "the biggest exercise since humankind came into existence". By early 2013, two years into the scheme, 300 million people had been enrolled – an impressive rate of progress which, if maintained, should see over 90 percent of Indians within the programme by the end of the decade.

Even so, technical problems with India's rollout have informed China's own scheme, a fingerprint-based national ID card system which was launched in early 2013. In particular, the Indian government has experienced difficulties "while enrolling citizens [who] are still not ready to share their full details due to a lack of trust in data management through electronic systems", explains Karan Chechi, Reseach Director at TechSci Research. But China, Chechi adds, has the advantage of having "already implemented biometric technology in various applications", notably in physical access control and attendance systems used by government departments.

China is also in a better position to draw on home-grown technologies, Chechi explains. "India has been largely focused on importing these biometric technologies, where many overseas vendors are involved," he says. In contrast, "home manufacturers are contributing heavily in China's biometric market," notably ZK Technology, which "has the highest share in terms of revenue for the biometric technology being manufactured" within China,

according to Chechi. Indeed, China has a vibrant biometrics industry. The Chinese Academy of Science's Institute of Automation (CASIA) has a Centre for Biometrics and Security Research, which now boasts laboratories and R&D facilities which rival those in Japan and the US.

The ambitious uptake of these technologies in Asia will come as a relief to a biometrics industry which has not taken off as quickly as many analysts had anticipated over the last decade. This resulted in a wave of consolidation, with major players such as Morpho (a unit of French technology firm Safran) and 3M (whose biometric arm is now called 3M Cogent) swallowing up niche biometric technology developers. Alongside these two, Chechi now ranks ZK Technology, South Korea firm Suprema Inc., and Japan's Fujitsu as the leading industry participants.

However, the slow early traction was caused in part by the technology's immaturity: accuracy is now much improved, even as developers are finding innovative new applications for biometric technology. These new applications are creating opportunities for customers and developers alike. "Continuous biometrics" is one such growth area Liu identifies whereby operators of privileged systems, either at a government facility or at a company handling sensitive data or materials, can be authenticated not just once when they log in, but continuously as they use the console. Smart video surveillance is another big opportunity for biometrics firms, Liu continues, pointing to the large numbers of CCTV cameras already installed in cities throughout the world. "Face recognition can potentially be conducted by matching every individual in the video with a 'wanted list'," he explains. "This can be done either in an online fashion, or as post-event forensic analysis, such as with the recent Boston bombing."

But ultimately much of the demand for biometric systems will come from the private sector. Any product or system which requires a log-in, or an ID card, or a secure payment, or even just an old-fashioned key may eventually incorporate some element of biometric identification. In China, for example, some employers are already using fingerprint recognition to enable workers to clock in and out – which gives the company a sense of added security about exactly who is on the premises. Many firms with security barriers at the entrance to their premises are also beginning to introduce biometric schemes: employees no longer have to carry swipe cards, and can access the building quickly and easily just by having their iris or fingerprint scanned.

Similarly, businesses such as gyms and health clubs are also beginning to adopt biometric ID systems to enable their members to access their facilities more quickly and conveniently than they could before – once again doing away with the old ID card, which is less secure and is prone to being lost. Further down the line, residential biometric security is also expected to start taking off, with individuals relying on their unique biometric signatures to secure their homes, their cars and their mobile devices.

New approaches are also opening up applications that were not previously considered. Vein recognition is the newest addition to the biometric stable, with Japanese firms such as Fujistu and Hitachi leading the field. "Vein technology is the new and trending biometric technology [because] the accuracy for acceptance is higher than other modalities available in the market," explains Chechi. Researchers are also now exploring the potential of DNA recognition, he explains. An effective DNA-based system would essentially increase the accuracy of biometric testing to 100 percent, making it particularly attractive for forensic and law enforcement agencies, Chechi says.

For the time being, ensuring total accuracy is not the priority for governments in China and India, which are focused instead on delivering high penetration for their historic national identity schemes. By the end of this decade, their efforts will see the transformation of biometrics from a fringe technology to an everyday system helping to run the world's two biggest societies. ■

Watch out!

HACKERS AT YOUR DOOR!

You may think that the threat of an electronic attack is receding; if you do, you'd be wrong. Attackers are just getting smarter, and perhaps they are at your door!

In March, the official website of the World Wide Fund for Nature (WWF) Hong Kong was hacked. Approximately fifty thousand personal data files might have been stolen and it's estimated that over ten thousand people were affected. Then on April 23, The Associated Press' Twitter account was targeted by hackers who tweeted that the White House had been attacked and President Obama injured. This led to a 143-point fall in the Dow Jones Industrial Average and wiped out US$136 billion from the S&P 500 index in just two minutes.

In fact we are not innocent bystanders; sometimes we are architects of our own downfall thanks to clever and not-so-clever tactics. A large number of targeted attacks frequently rely on social methods to compromise people, not just computers. We've seen examples of corporate security programs that are bypassed as a result of social tricks. Likewise, we've also seen actors go after high-value targets in their personal lives, using phishing, doxing, and watering hole attacks to compromise personal e-mail accounts and computing devices. There was an example in the US where a large retailer sent out an all-staff email clarifying

that at no time would employees be asked for their sensitive log-in details by the company – over 50 employees replied with their username and password details!

Asian people are technologically-savvy, plugged-in and receptive to social media platforms and new technology, but this also means that they could easily be at risk on the internet. As we have found, no one is immune.

What's happening?

Six years ago Verizon launched its first Data Breach Investigation Report (DBIR). The primary goal was to increase awareness of global cybercrime in an effort to improve the security industry's ability to fight it, while helping government agencies and private sector organisations develop their own tailored security plans. The report analyses data from law enforcement agencies, incident reporting/handling entities and other incident response firms, as well as Verizon's own dataset to compile the most comprehensive global report into adversary motives and methods.

This year, Verizon partnered with 18 different global organisations that study and combat data breaches. These organisations contributed a huge amount of data to the report; over 47,000+ reported security incidents and 621 confirmed data breaches from the past year. This gives Verizon a much more comprehensive, diverse dataset that is more reflective of what's really going on.

So what did the 2013 DBIR reveal? Launched in April, this year's DBIR revealed that large-scale financial cybercrime and state-affiliated espionage dominated the security landscape in 2012, at 75% and 21% respectively. In terms of financially-motivated attacks these were mostly targeted where the money is: financial institutions (37%), with retailers and restaurants (24%), manufacturing, transportation and utilities (20%) and information and professional services (20%) not far behind. Of all attacks, 38% impacted larger organisations and represented 27 countries.

However, what was even more telling for 2012 was the rise in state-affiliated attacks, which appeared in the number two spot for the first time. These include cyber threats aimed at stealing intellectual property (IP) such as classified information, trade secrets and technical resources to further national and economic interests. State-affiliated actors tied to China were the biggest movers in 2012. Their efforts to steal IP comprise about one-fifth of all breaches in this dataset.

External attacks also remain largely responsible for data breaches, with 92% of them attributable to outsiders and 14% committed by insiders. This category includes organised crime, activist groups, former employees, lone hackers and even organisations sponsored by foreign governments. As in the prior year's report, business partners were responsible for about 1% of data breaches.

In terms of attacking methods, hacking is the number one way breaches occur. In fact, hacking was a factor in 52% of data breaches.

- 76% of network intrusions exploited weak or stolen credentials (username/password);
- 40% incorporated malware (malicious software, script, or code);
- 35% involved physical attacks (such as ATM skimming);
- 29% leveraged social tactics (such as phishing).

Finally, third parties continue to detect the majority of breaches (69%), which means organisations don't even realise until it has been pointed out to them.

What can we do about it?

Some organisations will be a target regardless of what they do, but most become a target because of what they do (or don't do). If your organisation is indeed a target of choice, understand as much as you can about what your opponent is likely to do and how far they are willing to go.

Picking over the remains of data breach victims might paint a grim picture of our current state, but it's not a hopeless one. We have the tools, but it's selecting the right ones and using them in the right way that is important. To that end, we're convinced of the critical importance of understanding your enemy. If handling payment cards is your business, then there's a narrowly defined set of controls on which you can focus. If your IP is a hot commodity, you've got your work cut out for you, but knowing the attack patterns (and sharing them) can make that work more fruitfully. Take steps to better understand your threat landscape and deal with it accordingly.

Verizon recommends that com-

Countries represented in combined caseload

panies and individuals consider the detection of failures (in a reasonable time frame) as a success. The security industry has long been overly focused on prevention. Let's keep preventing, but enhance our ability to detect threats that slip through our defences (which they will inevitably do). For example, you can:

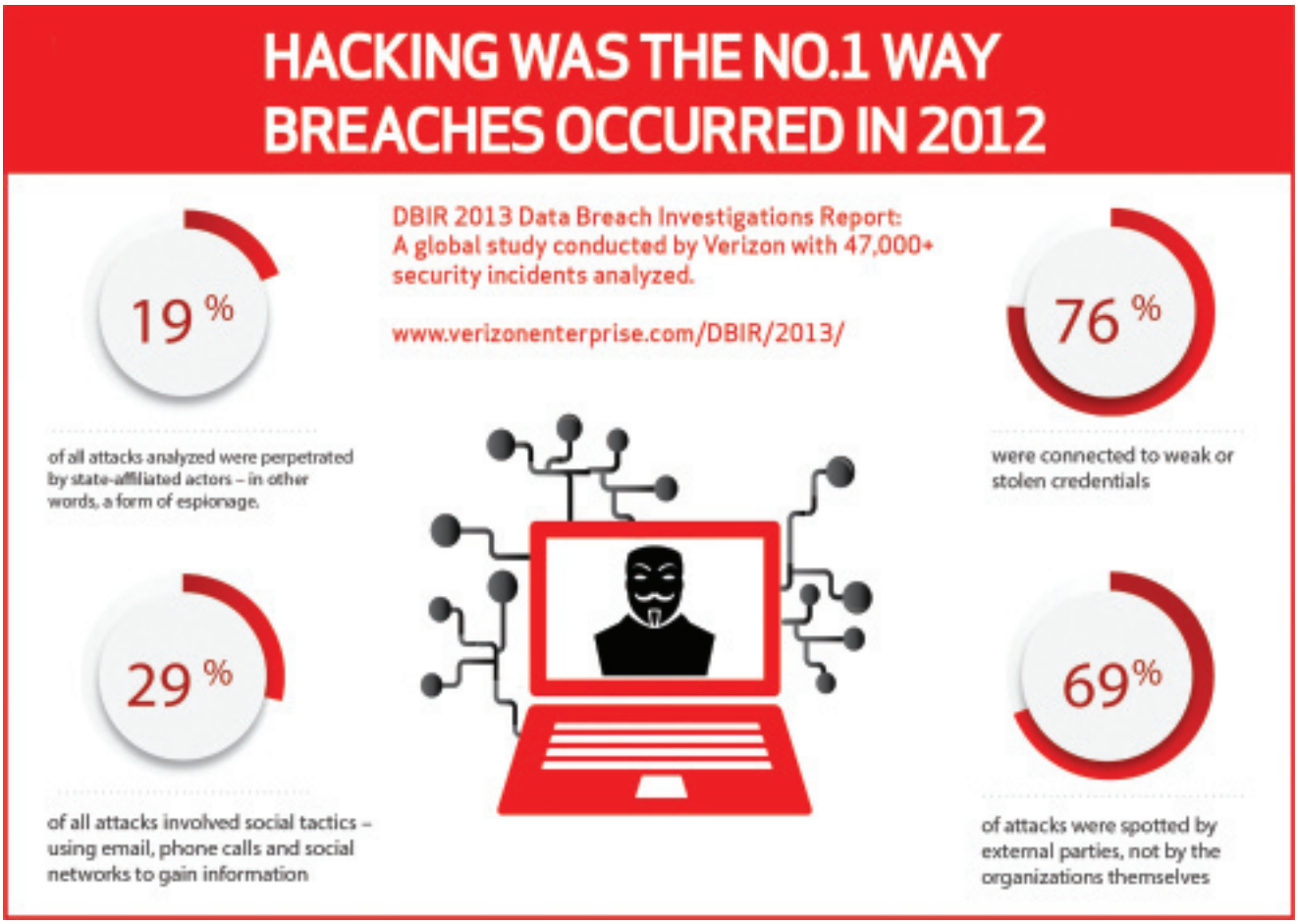
- Eliminate unnecessary data, and keep tabs on what's left;
- Ensure essential controls are met, and regularly check that they remain so;
- Collect, analyse, and share incident data to create a rich data source that can drive security program effectiveness;
- Collect, analyse, and share tactical threat intelligence, especially Indicators of Compromise (IOCs), that can greatly aid defence and detection;
- Without de-emphasising prevention, focus on better and faster detection through a blend of people, processes, and technology;
- Regularly measure things like "number of compromised systems" and "mean time to detection" in networks. Use them to drive security practices;
- Evaluate the threat landscape to prioritise a treatment strategy. Don't buy into a "one-size fits all" approach to security;

Staying alert to attack

The battle against cybercrime is ongoing, and attackers have their eyes firmly on the prize of the rich data that financial institutions and companies hold. To reduce your risk, businesses need to implement the basic tenets of an information risk management program and maintain this initial investment over time. This includes your network and your data defence technology basics such as firewalls; anti-virus technology; vulnerability management, identity and access management, as well as the non-technical aspects of security and risk management policy and process development.

Whatever you believe about angels and demons, cybercrime certainly exists. Don't believe for an instant that it will go away. Act now before it's too late! ■

By Claudio Scarabello
Senior Consultant
Verizon Enterprise Solutions



ASIS ASIA-PAC

7TH ASIA-PACIFIC SECURITY FORUM & EXHIBITION

MACAU, CHINA | 3-5 DECEMBER 2013

6 Reasons to Attend Asia-Pacific 2013!

1. **Industry leaders** from important companies and organisations will speak about the latest developments, trends and innovations in security.
2. **Apply lessons learnt** from other industries to your own sector.
3. **Connect** with high-level security professionals from all over the Asia-Pacific and beyond.
4. **Get motivated by** new ideas and information.
5. **Form new partnerships** and reconnect with familiar faces in the industry.
6. **Get social** and join discussions on Facebook, LinkedIn and Twitter

FEES	Early Rate until 4 November 2013	Regular Rate after 4 November 2013
ASIS Member	USD 995	USD 1,150
Non Member	USD 1,295	USD 1,500

CONTACT US asiapacific@asisonline.org
T.+32 2 645 2674 | www.asisonline.org/macau

SPEAKERS INCLUDE

TORSTEN WOLF
Group Head of Crime and Fraud Prevention; Zurich Insurance Company; Switzerland
A FRAMEWORK FOR MANAGING CRIME AND FRAUD

SUMMARY
Enterprises are increasingly confronted with the challenging task to protect their assets and their reputation. Especially companies that operate across the globe find it extremely difficult to protect their operations from criminals and fraudsters effectively and in a consistent manner. With reference to Zurich's comprehensive anti-crime framework the audience will get an understanding of crime and fraud risks an insurance organization typically faces, and can then reflect on how components of this framework may help enhance the fraud control environment within their own organizations.

PRAMOD BHATT
Vice President Protective Intelligence, Corporate Security and Business Continuity; Deutsche Bank; India
KEY EMERGING EXTREMISM RISKS TO CORPORATE SECTOR IN SOUTH ASIA

SUMMARY
One of the key emerging risks is from perpetrators who lack formal affiliations with extremist. Such individual may enjoy relative anonymity and easily evade law enforcement agencies. They can take advantage of this situation to find employment that gives them access to company premises and can commit direct attacks against companies.

ASIS INTERNATIONAL
Advancing Security Worldwide®

ENTRY TO THE EXHIBITION IS FREE OF CHARGE FOR PRE-REGISTERED VISITORS

Combating Crime as a Service

CCTV – PAST, PRESENT AND FUTURE CHALLENGE

CCTV is no longer just a passive tool to provide proof of crime after the incident – it now plays an active part in combating crime. CCTV has evolved from a simple hardware system to being a service-oriented solution: 'combating crime as a service'.

Analogue: older systems, lack of detail

Low resolution analogue images result in the absence of useful detail. This is one reason why analogue CCTV system in the past could only perform the functions of deterring and detecting crime, with limited effectiveness in the areas of facial recognition and the identification of critical details.

The present situation: IP versus HD-SDI

To obtain High Definition (HD) image quality, there are two possible options: IP surveillance or HD-SDI (High Definition Serial Digital Interface).

From the customer point of view, as IP surveillance operates over IP based networks, this means a totally new investment for analogue users.

With high resolution image quality, one HD-SDI camera can replace up to five analogue cameras, and as HD-SDI can run over existing coaxial cables used for the old analogue system, this option is attractive to users who wish to protect their investment in the current cabling structure. Moreover, as far as suppliers are concerned, traditional CCTV companies accustomed to analogue technology are unlikely to have IP expertise. HD-SDI is thus a viable direct upgrade solution for companies with old analogue systems not yet ready to opt for IP surveillance.

Mr. Benjamin Pflaum, Managing Director of ABUS.

Challenge: the downside to IP

IP surveillance systems can be potential targets for hackers. Anti-DDoS attack, anti-virus programs and many other measures typical to IP networking are relevant to IP surveillance.

IP system integrators selling the routers, switches and servers required for IP surveillance systems may not be fully aware that they require a valid security licence in Hong Kong to legally handle the design, maintenance and repair of CCTV security systems.

Combating Crime as a Service

The trend for CCTV systems to play a proactive part in combating crime may become more prominent once HD cameras, wireless devices and easily accessible high bandwidth transmission become widespread. CCTV customers will benefit from more added value from their security systems, not just through buying CCTV hardware but also from 'CCTV as a service' with customised, result-oriented vertical industry solutions that that will translate into 'combating crime as a service.'

Mr. Benjamin Pflaum is the Managing Director of ABUS. ABUS was founded 1924 in Germany and has a long tradition in developing high tech security solutions. The company is in favour of an open standard for interoperability and is a member of ONVIF, the organisation actively promoting IP CCTV product interoperability among vendors. ■

Drone On

China displayed an unmanned helicopter for the first time at the AVUSI (Association for Unmanned Vehicle Systems International) show in Washington in mid-August. The helicopter, known as the SVU-200 is made by China Ewatt Technology Co. Ltd. in Wuhan. Ewatt claims the helicopter to be 100% Chinese, although it is based on a design by Dennis Fetters, an American currently working in China as Ewatt's Technical Director of VTOL vehicles.

Fetters Aerospace, Mr Fetters' US company, recently signed a contract with Ewatt Technology to build a US$81 million dollar manufacturing facility for unmanned aerial vehicles in Wuhan. The deal represents the first venture between a US company and a Chinese company in civil drones, according to cnhubei.com and will tap into China's potentially huge UAV market.

The SVU-200 made its first flight in September 2012 and Ewatt expects to increase production from 200 units a year to 1000 units. Ewatt's Chief Executive Officer, Mr Zhao Guocheng says the company plans to build a line of VTUAVs (vertical take-off, unmanned aerial vehicles) over the next three to five years capable of carrying payloads ranging from 50 to 300 kg. The SVU-200 has a 78 horsepower engine and a top speed of 209km/h. It can lift a payload of up to 200kg and the company claims the vehicle requires less stability control inputs compared to similar helicopters.

Ewatt sent two of its drones to Lushan to record damage and help restore power after the Sichuan earthquake in April this year.

Geese police patrol Xinjiang

Is it a bird...; is it a plane...? Right first time – but who needs superheroes to fight crime when a flock of geese can be just as effective? Rural police stations in Xinjiang, Uygur autonomous region are recruiting geese to help guard the stations at night. You may consider this fowl play, but according to Hong Gang, the director of Dongwan police station, "Geese are highly vigilant, especially at night. They won't stop honking until the threat has gone and if one sounds the alarm the rest will follow." Duan Wencheng of Anjihai traffic police added, Of course, we also have surveillance cameras and infrared alarms, but they can be affected by the rain and other factors. The geese never make mistakes."

Geese have excellent eyesight and hearing and can be very aggressive to intruders. In fact, the guarding abilities of geese were documented in 390BC when holy geese in a temple alerted sleeping Romans to an attack by Gallic troops. The UN Food and Agricultural Organization have stated that in Europe they have been used to guard whiskey warehouses and sensitive military installations.

Although penned in by day for the safety of villagers, the Xinjiang geese roam the police compound by night, trimming the grass and watching for trespassers. But are their superiors tempted to look upon them as dinner? "We used to keep them for their eggs and meat," said Hong. "Now they have been promoted, we can't bear to eat them anymore."

Zhao Yufei / China Daily

New recruits goose-stepping past Dongwan police station

Network security market expected to grow

With the rise of cloud computing and the growing popularity of bring-your-own-device (BYOD) flexibility, companies are becoming increasingly concerned about the risks of hacking. The concern is not only from the point of view of financial and intellectual property loss, but also from the adverse publicity and loss of confidence that successful attacks generate.

Businesses now have to ensure their networks are fully protected and also guard against content and application-layer attacks such as distributed denial of service (DDoS). This has led to a demand for software developers and manufacturers and distributors of network security systems throughout the region. In 2012 the Asia-Pacific network security market grew by 5.7% and earned US$2.16 billion, according to market research firm Frost & Sullivan.

Meanwhile, documents leaked by US whistleblower Edward Snowden in relation to NSA intelligence gathering, and in particular the PRISM project, may have harmed US technology companies to the tune of US$22 to $35 billion over the next three years according to the Information Technology and Innovation Foundation (ITIF) in Washington. A survey by the Cloud Security Alliance found that 10% of its non-US members had cancelled a project with a US-based cloud computing service and 56% were less likely to choose a cloud computing provider in the US as a result of Snowden's NSA disclosures. Over a third of its US members indicated the leaks made it more difficult for them to do business outside the US.

Information and communications tech-nology companies in the Asia-Pacific region have an unprecedented opportunity to seize on the leaks and economic woes affecting the US and Europe and surpass the US$3.62 billion in revenue projected by 2018.

North Korean smartphone with Chinese characteristics

This month, North Korean state media released pictures of leader Kim Jong-Un inspecting a smartphone apparently made at a North Korean factory. The 'Arirang' features all the goodies you would expect from a modern smartphone, including a touch screen, a high-resolution camera and Google's Android operating system. However, technical experts remain dubious. Whilst most believe that the North Koreans are capable of building a smartphone, doubts remain over the North Koreans' ability to provide the hardware. Kang Ho Jye of the Ewha Institute of Unification Studies, Seoul, South Korea, noted that 'If people believe it is impossible for North Korea to make smartphones because it lags in technology, that's not right. If people believe it is impossible because they are wondering how North Korea supplied components, then that makes sense.'

Moreover, North Korea watchers also point to the fact that photographs released by the Korean Central News Agency (KCNA) only show workers testing and packing the finished phone. There is no evidence of assembly lines or machines in operation. Martyn Williams, who operates the northkoreatech.org website, writes "...they are probably made to order by a Chinese manufacturer and shipped to the May 11 Factory where they are inspected before going on sale.

Earlier this year the number of North Korean mobile users rose to 2 million, according to South Korean news agency Yonhap. North Korean wireless provider Koryolink does not offer international calls or internet access, and all domestic calls are monitored by the authorities. A closed intranet allows a limited number of users to exchange state-approved information. On his recent factory tour, Kim Jong-Un noted approvingly that the Arirang 'provides the best convenience to the users while strictly guaranteeing security.' However, smuggled Chinese cell phones allow a few North Koreans living close to the border illicit access to the outside world.

KCNA

Kim Jong-Un inspects the Arirang Smartphone

‘World’s smallest mobile’ may be banned in UK

The UK government is consulting the Serious Organised Crime Agency and the National Trading Standards Board (NTSB) about banning the sale of tiny cell phones made to resemble car key fobs over fears they could easily be smuggled into prisons. The Chinese-made key fobs bear the logo of car brands such as BMW, VW and Porsche and are outwardly similar to the fobs used to lock and unlock car doors. Moreover, they are constructed largely of plastic and are easily concealed, making them difficult for prison security systems to detect.

In the UK, possession of a mobile phone in prison carries a 2-year jail sentence and/or an unlimited fine. Prisoners are allowed calls to cleared numbers from public phones in prison wings to contact their families and these may be monitored. The restrictions aim to prevent inmates from bullying witnesses, contacting victims or any other person the authorities deem inappropriate.

The police have urged car manufacturers to take up the issue of copyright infringement and the NTSB are urging retailers to refrain from selling the items. The prison service’s recent deployment of high sensitivity metal detectors and body orifice security scanners has seen the number of seizures increase and there are moves to block cell phone signals within prisons.

At the time of going to print, Security Asia found that Amazon had withdrawn the fob phones, although they were still available on Alibaba and eBay priced between US$20 and US$70.

Detention and computer wrecking mark latest twist in Snowden saga

Questions have been raised regarding the detention of David Miranda, a Brazilian citizen, for almost nine hours at Heathrow airport under schedule 7 of the Terrorism Act. Mr Miranda is the partner of Glenn Greenwald, the journalist that interviewed NSA whistleblower Edward Snowden for the UK newspaper The Guardian. During his detention, Mr Miranda’s electronic equipment, including his laptop, camera, memory sticks and games console, was confiscated by officials. Mr Miranda was en route from Berlin to his home in Rio de Janiero when he was stopped.

The purpose of Schedule 7 of the Terrorism Act is to determine whether or not a person is engaged in terrorist activity and only applies to airports, ports and border crossings. Nine hours is the maximum length of time an individual can be held without being charged.

Fearing public support for schedule 7 would be undermined by inappropriate use, the shadow home secretary, Yvette Cooper, said "Any suggestion that terror powers are being misused must be investigated and clarified urgently. ”Mr Greenwald called it an attack on press freedom and claimed the detention was “clearly intended to send a message of intimidation to those of us who have been reporting on the NSA and GCHQ.” Meanwhile, Brazil voiced ‘grave concern’ about the detention of one of its citizens under the UK’s anti-terror laws.

So far Scotland Yard have only issued a brief statement confirming Mr Miranda’s detention and release without arrest.

In a related development, senior Guardian staff used angle grinders and drills to destroy computer hard drives and memory chips under the watchful eyes of GCHQ technicians. The storage devices contained copies of files leaked by Snowden, and although The Guardian editor, Mr Alan Rusbridger, informed the government that the files existed outside the UK and that the newspaper was neither sole recipient nor steward of the files in question, officials insisted on destruction or surrender of the stored files.

The decision to destroy the material was taken to avoid betrayal of the source (Snowden) and to protect journalists who may have worked with the files from being identified through forensic analysis. Rusbridger also believed that if the UK government sought to prevent UK reporting of Snowden leaks, then the best option would be to destroy the London files and continue the work in Brazil and America protected by the first amendment guaranteeing free speech.

Subscribe to SecurityAsia Today!

Yes please, I would like to get a free subscription for Security Asia.

Name:

Job Title: **Email:**

Company Name:

Address:

Country:

Please print in block capital letters

Send your form to us by:
Scan and **email** this form to Circulation@RRPublishing.com.hk *or* **fax** this form to +852 2126 7816
or **mail** to R&R Publishing Limited, 705, 7/F, Cheong K. Building, 84-86 Des Voeux Road Central, Hong Kong

Order your free subscription and have *Security Asia* delivered straight to your desk or home.

Essential reading for everyone involved in security.

Careful with that app., Eugene

According to Kaspersky Lab's IT Threat Evolution Report for Q2 2013, Android-based malware is becoming the mobile equivalent to Windows PC malware as cybercriminals build on their knowledge of PC malware to expand and develop malicious programmes for mobile platforms. Android is the obvious target, as around 80% of smartphones use this OS. One common technique is for cybercriminals to download a legitimate mobile application and modify it with a malicious code. The infected application is then uploaded to third-party app stores frequented by smartphone users attracted to free downloads.

By the end of June this year, Kaspersky Lab had identified over 100,000 modifications to mobile malware, with backdoor Trojans overtaking SMS-Trojans in terms of modifications added.

The most sinister Trojan yet discovered, Backdoor. AndroidOS.Obad was able to steal information about the infected smartphone and its apps, send SMS messages to premium numbers and spread malware via Bluetooth. The code clouding techniques employed to avoid detection were the most advanced yet.

Another notorious Trojan, Ransomeware, made its appearance on Android as Free Calls Update in June when it was downloaded from third-party stores. Once installed, it attempted to gain administrator rights and change the phone settings. The app. then pretended to find malware and instructed the user to buy fake virus removal software whilst blocking user access to the phone.

At present, Android infection rates for mobile devices are very low and if you avoid dubious third party sites and suspect free apps. the chances of wrecking your smartphone are remote. However, cybercriminals are shifting their focus away from traditional PCs and will find new ways of distributing increasingly sophisticated malware.

Syrian Electronic Army marches on Washington Post

Recently, the Syrian Electronic Army (SEA) was able to compromise a website belonging to the Washington Post. In a blog dated 15 August, Washington Post Managing Editor Emilio Garcia-Ruiz acknowledged the SEA launched what he termed 'a sophisticated phishing attack to gain password information.' The attack resulted in a staff writer's Twitter account sending out a SEA message and caused the Post's website to redirect some readers to the SEA website. The hacking attack actually targeted Outbrain, a third-party content discovery platform used by The Washington Post and the service was taken down once the breach was noticed, around 30 minutes later. Experts noted that the attack differed from the China-based hacking attack on the New York Times as it targeted users rather than attempting to acquire internal information. If users' believe their own computers are at risk from malware, they may be inclined to avoid such breached sites in future.

The Syrian Electronic Army claims to be a group of patriotic youths sympathetic to the government of Syrian President Bashar al-Assad. It attempts to promote a political agenda by breaching high profile websites.

Insurance companies set to profit from cybercrime

A recent study conducted for the insurance industry by Experian Data Breach Resolution and the Ponemon Institute found that almost three-quarters of businesses surveyed consider cyber security risks to be an equal or greater threat than any other risk, including fire and natural disaster. Less than one-third of respondents were covered by cyber risk insurance, although over half of those without insurance planned to take out a policy in the near future.

With data breaches costing companies and average of US$9.4 million over the last two years, and potential losses far exceeding $100 in some cases, it is no wonder interest in cyber risk insurance is escalating. The survey findings led the researchers to predict 100% growth in cyber risk policies purchased within two years.

Software sends virtual humans running for the exits

A computer programme developed by Luciano Soares and students at the Polytechnic School of the University of São Paulo may help planners design safer buildings in the event of fire or other emergency, according to *NewScientist.com*. The programme places virtual humans in a virtual building and requires them to hasten for the exits in response to some threat. By varying the number and the fear level of the virtual victims and the type of threat, Soares' team are able to simulate how groups of people might react in an emergency.

A version of the programme installed on a tablet computer uses the tablet's camera to film the rooms and passageways of a real building in real time and superimposes the virtual humans rushing for the exits. This may assist in the identification of local bottlenecks such as narrow doorways and corridors.

London's 'smart bins' canned

If you walked through central London in the past year, there's a good chance a recycling bin noticed you passing by. The bins were installed by a company called Renew London and have LCD panels displaying advertising to the City's affluent workforce. Controversially, a dozen of them also collected the MAC address from any passing smartphone that happened to have its WIFI enabled.

Over the course of one week, the company reportedly captured over 4 million devices. With a tracking cookie placed on the smartphone, the company would be able to collect information regarding a person's movements and sell it to potential advertisers, allowing brands to tailor their adverts to individuals. As the bin records your habits and preferences, rival brands could remind you of their offers as you stroll down the street. Starbucks or Costa Coffee...the bin might have a suggestion for you.

With growing public concern over privacy, The City of London has referred the issue to the Information Commissioner's Office. Renew also confirm that they have stopped collecting data in response to a request from the City. CEO Kaveh Memari states on the company website "A lot of what had been extrapolated is capabilities that could potentially be developed but none of which are workable right now. We no longer continue to count devices and are presently not able to distinguish uniques versus repeats."

Industry Events

3rd Annual Information Security Summit
Reducing Vulnerabilities, Securing Business
3-4 Sep, '13
The Royale Chulan Hotel, Kuala Lumpur, Malaysia
www.asianworldsummit.com/AWS/AWS_Event_3rd_ISS.html

7th Asia-Pacific Security Forum & Exhibition
3-5 Dec, '13
Conrad Macao Cotai, Macau, China
www.asisonline.org/Education-Events/Global-Conferences/asia-pacific/Pages/default.aspx

Course

The Critical Infrastructure Protection Training (CIP)
4-8 Nov, '13
Singapore
www.ib-consultancy.com/events/event/48-critical-infrastructure-protection-training-cip.html

SEC440: 20 Critical Security Controls
17-18 Sep, '13
Malaysian Communications and Multimedia Commission
Prima Avenue One, Block 3507, Jalan Teknokrat 5, Cyberjaya
Malaysia
www.sans.org/event/sec440-mcmc-2013

The Critical Infrastructure Protection Training (CIP)
4-8 Nov, '13
Singapore
www.ib-consultancy.com/events/event/48-critical-infrastructure-protection-training-cip.html

Seminars and Conferences

International Conference on CyberCrime and Computer Forensic 2013
Build a Secure Cyberspace 2013
25-28 Aug, '13
Crowne Plaza Hong Kong Kowloon East Hotel, Tseung Kwun O, Hong Kong
www.apccf.org

Cyber Security Symposium 2013
Share to Win – Build a Secure Cyberspace
30 Aug, '13
Gallery Room, G/F, Police Officers' Club, 28 Hung Hing Road, Causeway Bay, Hong Kong
www.hkcert.org/my_url/en/event/13083001

The Non-Conventional Threat: CBRNe Asia 2013
24-27 Sep, '13
Aloft Hotel, Kuala Lumpur, Malaysia
www.ib-consultancy.com/events/event/41-cbrneasia.html

S2 Institute Anti-Terrorism Officer Seminar
7-10 Oct, '13
Concord Hotel, Orchard Road, Singapore
www.s2institute.com/content/_pages_advanced/_courses/ato_singapore13.php

NCT C-IED Asia 2013 – The Asian EOD and IED Forum
29 Oct-1 Nov, '13
St. Regis Hotel, Bangkok, Thailand
www.ib-consultancy.com/events/event/43-nct-c-ied-asia.html

Cyber Security and Digital Forensics
3-5 Dec, '13
Le Méridien Hotel, Kuala Lumpur, Malaysia
www.ib-consultancy.com/events/event/44-cyber.html

Travel Advisory

When you are planning to travel on business or holiday please be aware that there are security travel warnings in place for many countries in the Asia Pacific area. We strongly advise that you contact your embassy/consulate to get the latest information/status on your destination country.

Hong Kong's official website of all embassies and consulates located in the territory can be found here:
www.protocol.gov.hk/eng/consular/index.html

The GoAbroad website will help you find any country's embassy or consulate around the world:
www.embassy.goabroad.com

Security Asia wishes you a safe and secure journey.

Who is behind data breaches?

- 98% stemmed from external agents (+6%)
- 4% implicated internal employees (-13%)
- <1% committed by business partners
- 58% of all data theft tied to activist groups

How do breaches occur?

- 81% utilized some form of hacking (+31%)
- 69% incorporated malware (+20%)
- 10% involved physical attacks (-19%)
- 7% employed social tactics (-4%)
- 5% resulted from privilege misuse (-12%)

What commonalities exist?

- 79% of victims were targets of opportunity (-4%)
- 96% of attacks were not highly difficult (+4%)
- 94% of all data compromised involved servers (+18%)
- 85% of breaches took weeks or more to discover (+6%)
- 92% of incidents were discovered by a third party (+6%)
- 97% of breaches were avoidable through simple or intermediate controls (+1%)
- 96% of victims subject to PCI DSS had not achieved compliance (+7%)

Where mitigation efforts should be focused Smaller organisations

- Implement a firewall or ACL on remote access services
- Change default credentials of POS systems and other Internet-facing devices
- If a third party vendor is handling the two items above, make sure they've actually done them

Larger organisations

- Eliminate unnecessary data; keep tabs on what's left
- Ensure essential controls are met; regularly check that they remain so
- Monitor and mine event logs
- Evaluate your threat landscape to prioritise your treatment strategy

Motive of external agents by percent of breaches

- Financial or personal gain: All Orgs 96%; Larger Orgs 71%
- Disagreement or protest: All Orgs 3%; Larger Orgs 25%
- Fun, curiosity, or pride: All Orgs 2%; Larger Orgs 23%
- Grudge or personal offence: All Orgs 1%; Larger Orgs 2%

Hacking methods by percent of breaches

- Exploitation of default or guessable credentials: All Orgs 55%; Larger Orgs 9%
- Use of stolen login credentials: All Orgs 40%; Larger Orgs 51%
- Brute force and dictionary attacks: All Orgs 29%; Larger Orgs 14%
- Exploitation of backdoor or command and control channel: All Orgs 25%; Larger Orgs 29%
- Exploitation of insufficient authentication (e.g., no login required): All Orgs 6%; Larger Orgs 3%
- SQL Injection: All Orgs 3%; Larger Orgs 14%
- Remote File Inclusion: All Orgs 1%; Larger Orgs 6%
- Abuse of Functionality: All Orgs <1%; Larger Orgs 3%
- Unknown: All Orgs 4%; Larger Orgs 31%

Source: Verizon DBIR 2013

Airport Security:

THE CHEESE BOMBER

"We've had shoe and underpants bombers...
... a fermented milk terrorist could well be the next imaginative step".

By Peter Sherwood

Question: Would you sacrifice your seat on a 12-hour flight home for a 250gram packet of soft cheese? To hazard a guess, you would not, but then you're not an irate man whose curdled treasure - along with his curdled dignity it seems - was quickly and ceremoniously confiscated by an Amsterdam official with an airport rule book.

Apparently the popular 'Philadelphia' product is listed in the ordinance under 'creams and jellies', enough to have it banned from flights (along with, I previously discovered, Vegemite and fine French marmalade).

Fair enough. We've had shoe and underpants bombers, so a fermented milk terrorist could well be the next imaginative step. The man was mad as hell and righteous enough to stand his ground (or airport terminal carpet) demanding his rights, and his cheese, when by law he had none of the former and would lose all of the latter, while missing his plane – on principle. I know because I sat on that flight back in July, almost as incensed as the cheese bloke while they unloaded his bags. He might be there still, fuming.

And all for a product that's easy to buy in Hong Kong - and contains enough 'bad' cholesterol to explode your arteries

What Cheeseman failed to understand are the intricacies of debating a Customs officer. The secret is 'don't'. Like wrestling a crocodile or falling into quicksand, the harder the struggle the more inevitable the outcome.

Airport security varies madly. At some it is demanded you remove your shoes, even flip-flops. Or your belt, watch, or Gothic nose and nipple piercings. You never know. Being suddenly disarmed like that can be, well, disarming, and can send some people into the irrational panic of the innocent. At a stretch that might be understandable.

What lies light years beyond comprehension is stuck at Kathmandu airport's 'Wish I Were Dead' arrivals area. Here sits a half-wrecked and antiquated security machine with a sign saying all bags must be X-Rayed and examined leaving the airport. (Or you can just bypass the machine with your luggage. The decision is arbitrary – and as irrelevant as the equipment). One might have the temerity to ask why (some) bags might be examined on the way out, after being scrupulously examined at the point of departure – and by equipment at airports that actually works. But that would be silly if only because I tried it once and was laughed at.

Arbitrary too was the procedure I went through years ago at Moscow airport on the way to a mountain trip. The entire city and its airport were in a state of rotting decline, except for the new state-of-the-art security gear; magnificent British-made stuff to explore every bag in detail. These machines were every bit as severe on passengers as their surly operators. Our bags passed muster and we walked untroubled to the plane - each carrying a large pair of sharp pointed crampons and an ice axe. ■

Peter Sherwood is a long-term Hong Kong resident. For eight years he wrote a regular satirical column for the SCMP. He is the author of 15 books.

Security Asia magazine can help grow your business!

It's a bold claim – so how can we help you?

Here's how:

- We'll keep you informed of the latest developments and trends in the security industry with feature articles written by experts.
- We present new and interesting products with our regular 'Latest Security Devices' article.
- If your company has a unique product or service, tell us about it and we may showcase it in an editorial.
- Security Asia is read by over 10,000 professional people directly related to the security industry. It is mailed to senior executives and decision-makers who choose to purchase products and services.
- We can work together to promote your business to exactly the right people.
- No other local magazine gives you access to the region's security elite.

Call Colin on (852) 2126 7812,
email Advertising@RRPublishing.com.hk
or visit our web page
www.Security-Asia.net/advertise-with-us
to find out how we can help grow your business.

For more information about *Security Asia*, please visit our website, www.Security-Asia.net

SecurityAsia is delivered directly to associations and decision makers who are responsible for purchasing security related services and products including:

- Members of The HKSA
- Government security bureaus
- Security consultants
- Law and accountancy firms
- Financial institutions
- Insurance companies
- Transportation companies
- Facilities management providers
- Security hardware and software manufacturers

Security Asia is the only magazine published in Hong Kong for the security industry and endorsed by The Hong Kong Security Association. It is distributed throughout the Asia-Pacific region.

R&R PUBLISHING

R&R Publishing Ltd
705, 7/F, Cheong K. Building, 84-86 Des Voeux Road Central, Hong Kong
Tel: (852) 2126 7814 Email: Advertising@RRPublishing.com.hk
Web: RRPublishing.com.hk

The ASA Group

Security & Aviation

www.asag.aero

Specialist providers of trustworthy private aviation and VIP security services throughout the Asia Pacific region

- **Full Ground Handling, Supervisory and Coordination Services**
- **Landing & Overflight Permits**
- **Private Charter Flights**
- **Secure Transportation for Crew and Passengers**
- **VIP Executive Protection and Security Services**

For more information, please call Joe Wilson on +852 9866 6764
Email: enquire@asag.aero
Website: www.asag.aero

Hong Kong | Macau | China | Taiwan | Thailand | Cambodia | Laos | Vietnam
Myanmar | Singapore | Malaysia | Indonesia | Philippines | South Korea | Japan