CYBER IQ

# CYBERSECURITY REVIEW

## *SUMMER 2016*

www.cyberiq.co.uk

# CONTENTS

FOREWORD 4
Richard de Silva, Editor, Cyber IQ

EVERY ORGANIZATION IS A TARGET: THE PERVASIVENESS OF RANSOMWARE 7
Insight from threat research expert, Ryan Lai

CREATING AN INFOSEC CULTURE 11
Insight from Chris Rivinus, Head of IT Finance at Tullow Oil

CYBER IQ SUMMER SURVEY 15
Insight from the international IT security community

HACKING TEAM FALLOUT 21
*Who can we trust?*

INTERVIEW: GOVERNMENT-LEVEL CYBERSECURITY 25
Insight from Baroness Neville-Jones, Former Minister of State for Security (UK)

THE 'MR. ROBOT' PROPHECY 28
*Will a cyber attack cause a global meltdown?*

THE PERFECT PR PLAYBOOK 32
*Saving your reputation after a cyber attack*

INDUSTRIAL SYSTEMS: OT-IT CONVERGENCE 35
*Is it inevitable?*

INTERVIEW: CYBER RISK FOR FINANCIAL SERVICES 39
Insight from Peter Mitic, Head of Operational Risk Methodology, Banco Santander

PROTECTING FINANCIAL DATA FROM INSIDERS 44
With insight from banking security risk expert, Patrik Heuri

Informationsecurity FS

**25-27 October, 2016 | London**

## Information Security Financial Services

Entering its **5th year, the Information Security FS** Conference is the premier opportunity for cyber security discussions designed specifically for financial services organizations. The event will be hosted in London on the 25th – 27th October 2016.

As the sector that attracts the most cyber crime globally, 38% of financial service firms said that they would be spending to combat threats over the next 12 months, and globally it is predicted that the sector will increase its spending by $2 billion over the next 2 years.

In conjunction with this ever growing threat, the impending **General Data Protection Regulation** (GDPR) act being discussed within the European parliament (that could result in fines of up to 5% of the global turnover) alongside existing PSD2 legislation makes the compliance framework more complicated than ever, meaning cyber security must be at the forefront of the financial service industries mind.

Information Security for Financial Services is the premier opportunity in Europe for financial services cyber security stake holders and solutions providers to gather and discuss the strategic, technical and risk considerations of their information security policy. Information Security FS provides an unmissable opportunity to discuss the threats of today and the issues of tomorrow with the most like-minded audience available.

**WWW.INFOSECFS.COM**

**enquire@iqpc.co.uk** **+44 (0) 207 036 1300**

# FOREWORD

## By Richard de Silva, Editor, Cyber IQ

Welcome to the summer 2016 issue of the Cyber IQ Review.

The past few months have been as active as ever when it comes to the increase and emergence of sophisticated threats to our digital information. Headline issues have spanned from flaws in daily security measures to global-scale controversy and serious commercial fallout.

The latest research by best practice solutions provider AXELOS claims that organizations in the UK are generally failing to teach their employees cybersecurity, resulting in significant gaps in their virtual defences. Most methods being used now – such as computer-based training and e-learning – are believed to be outdated, while knowledge shared through these methods is often quickly lost. In short, annual e-learning courses are not enough to promote resilience.

Similar observations have been made by other experts decrying a blanket reliance on conventional wisdom. For example, the concept of changing one's password on a regular basis has long been advisable in order to maintain low-level security, but the importance afforded to this action over the years has overhyped its potency, inadvertently creating a very common false sense of security. Today's advanced threats – of which there are many – can of course overcome the hurdle of passwords easily.

Likewise, solutions providers offering tools that solve all of life's cybersecurity problems are often bought, applied and forgotten. Aside to the fact that most tools cannot cover every layer of security required, those building them into their businesses are often overconfident in their power, do not know how to validate their capabilities, and forego regular training, updates, or other measures of resilience.

> 2015 saw more than 100 million healthcare records compromised – and those are just the ones that were reported.

The risks of poor security training are of interest because almost every senior manager of a modern business will claim that security training for staff is essential. However, the studies show that less than half are modifying training over time.

At a wider level, new research from IBM has found that five of the eight largest healthcare cybersecurity breaches since 2010 (those with more than 1 million records reportedly compromised) occurred in 2015. Overall, that year saw more than 100 million healthcare records compromised – and those are just the ones that were reported.

If the research is accurate, this puts healthcare at the top of the list of industries for number of cyberattacks. Industries following close behind are understood to be manufacturing, financial services, government and transportation, respectively.

Other sources cite nine 'mega-breaches' across the year, resulting in the theft of over 420 million records of financial and personal information.

Perhaps one of the most interesting recent findings from IBM's assessment is that sixty percent of cyberattacks in 2015 were the result of an insider using physical or remote access to an organization's assets. This does not just consist of employees, but also of third parties, such as business parties or maintenance contractors. Arguably, there is too much trust being doled out rather than basic security procedures, such as network segmentation, temporary user restrictions or continuous monitoring.

> The San Bernardino/iPhone debate has brought the issue of zero-days, ethics, and private-public collaboration to the mainstream.

Also on the rise last year, according to a Symantec study, were exploits of zero-day vulnerabilities, of which the known tally (54) more than doubled the previous record set by 2014. This is presenting a problem for both programmers and law and intelligence agencies. The time taken to close zero-days is believed to be dropping, but market demand (for either criminal or counter-criminal purposes) is playing a part in their increasing discovery. In one of the biggest cybersecurity stories of the year, the San Bernardino/iPhone debate has brought the issue of zero-days, ethics, and private-public collaboration to the mainstream.

As far as global cybercrime is developing, Symantec sees cybercriminals adopting corporate best practices and establishing professional businesses in order to increase the efficiency of their attacks against enterprises and consumers. The pin has been placed on India as the world's top destination for cybercrime worldwide, with 15 ransomware attacks targeting systems within the country every hour.

This e-book includes new insight from experts within the field of information security, including strategic expert Ryan Lai on ransomware, and Dr. Chris Rivinus on developing an 'InfoSec culture'. Alongside these, we offer access to some of the most impactful articles that *Cyber IQ* has released in the past six months, covering elements from national infrastructure protection to incident response. Meanwhile, readers will be able to find the results of our summer survey of cybersecurity professionals, in which we uncover some interesting trends and statistics, including what they believe to be the most critical vulnerabilities and where organizations are failing on implementing policies and procedures.

For those new to the name, *Cyber IQ* has been conducting some of the world's leading cybersecurity conferences for over ten years. Our annual calendar includes *Cyber Defence and Network Security (CDANS),* the trans-European *ICS Cyber Security* series, *Information Security for Financial Services* (coming this September), and *Cyber Intelligence, Resilience and Response* (November). Should any of these appeal, readers are welcome to contact us to book a place.

While we hope you take away something useful from these materials, we also encourage further input and, indeed, counterpoints. If you have a perspective that you believe needs to be shared with the cyber security community, we would be delighted for you to get in touch.

## REFERENCES

AXELOS:
http://www.itproportal.com/2016/04/18/uk-organisations-cyber-security-training-is-outdated/
IBM:
http://www.healthcareitnews.com/news/five-eight-largest-healthcare-cybersecurity-breaches-2010-occurred-2015
Symantec zero-day:
https://www.symantec.com/security-center/threat-report
India: http://www.ibtimes.co.in/india-remains-top-source-target-cyber-attacks-report-675585

**Richard de Silva** (BA, MA) is Chief Editor of the *Cyber IQ Review* [Summer 2016]. He reports on security and defence at *DefenceIQ.com* and is the head of online content. He is a regular face at leading trade show events, including Eurosatory, DSEi, Farnborough Air Show and the Counter Terror Expo, and has interviewed some of the world's most senior military leaders, including Gen Sir Peter Wall (British Army), Gen Mike Hostage (US Air Force), Lt. Gen. Michael Flynn (Director, US DIA), and Vice Admiral Rinaldo Veri (NATO; OUP naval commander). He also co-manages production of *Defence Industry Bulletin*.

# EVERY ORGANIZATION IS A TARGET: THE PERVASIVENESS OF RANSOMWARE

## By Ryan Lai, threat research expert, Cyber IQ

In February 2016, the Hollywood Presbyterian Medical Center in Los Angeles, California was the victim of a cyber attack that encrypted its electronic data rendering its systems unusable for over a week. The hospital was forced to operate with no access to its computer systems and even had to move some patients to other hospitals. Staff relied on fax machines and telephones to keep hospital operations moving. The hospital regained access to its data only after paying a fee of 40 bitcoin (approximately USD 17,000) to the attackers. In March 2016, Methodist Hospital in Henderson, Kentucky, experienced a similar attack and declared a "state of emergency" being unable to access patient files. Methodist Hospital was able to restore their system from data backups and did not pay the attackers.

In both instances, the hospitals fell victim to a family of ransomware called Locky. Ransomware is a type of malware that encrypts a victim's data and demands a ransom payment for the decryption keys necessary to restore access. The ransom is generally priced based on the lowest amount the attacker believes the victim will pay. Cyber criminals have become experts at pricing strategy – ransoms demanded of individuals can be as low as US $30, but into the tens of thousands for enterprises. Since 2014, the CryptoLocker ransomware family alone has allowed cyber criminals to collect over $100 million.

In today's connected enterprises, any temporary loss of data can be debilitating and lead to lost sales and halted productivity. *Permanent* loss of data, however, could be catastrophic. An enterprise could lose access to all sales records, customer files, ledgers, intellectual property, and more. The cost to restore such data from zero is far more than many companies could bear.

Such cryptor attacks are relatively inexpensive to develop and launch and as a result are becoming pervasive. Kaspersky Lab estimates over 750,000 users worldwide were infected by ransomware in 2015. The various ransomware families come and go, but the most ubiquitous include CryptoLocker, Cryptoxxx, TorLocker, TeslaCrypt, and CryptoWall targeting Window O/S, KeRanger targeting Mac OS and Linux.Encoder targeting Linux systems.

> It is very unlikely that a tool can be developed to universally help victims once the ransomware has executed.

The information security industry is devoting significant attention to these growing threats and have made some progress against specific ransomware families. In May 2016, Kaspersky Lab produced a free decryption tool for victims of Cryptxxx. Romanian endpoint security company Bitdefender has similarly created various decryption tools for some variants of Linux.Encoder. TeslaCrypt recently became obsolete as its authors released a master key which was used to produce a universal decryption tool by Slovak security firm ESET. Patrick Wardle of Synack created a utility (RansomWhere?) to block ransomware attacks on OS X by detecting and halting rapid encrypted file creation in home directories.

It is important to note that no one has, or likely can, break the actual encryption to recover the data. In the instance of Linux.Encoder, Bitdefender researchers found a significant flaw in Linux.Encoder which allowed them to extract the decryption keys that were generated on the victim machine. TeslaCrypt authors surprisingly volunteered the master decryption keys to the community which allowed ESET to build the decryption tool. So, while the security industry is making important strides in defensive research, it is very unlikely that a tool can be developed to universally help victims once the ransomware has executed and the encryption process has completed.

### What can you do about this?

To understand the defensive measures available, security practitioners should view a ransomware attack in three separate phases: pre-infection, mid-infection and post-infection...

### Pre-Infection

Two of the most common ways for attackers to launch a ransomware attack are by phishing and watering-hole/drive-bys. Phishing is where a victim receives an email that contains an infected attachment or a link to an infected website. Water-holing refers to attacks where the victim is a particular group and the attacker guesses or observes which websites they most often visit and infects the victim via drive by exploit.

*Educate your users.* People are the vulnerable element that allows these attack techniques to succeed. Teach your employees about IT security basics to include awareness of phishing risks and the security implications of opening any email attachment that looks suspicious or came from an unknown sender. Do not follow unsolicited web links in email. Attackers can send highly sophisticated phishing emails that are designed to appear legitimate, but the majority of phishing attempts should be discernible to an employee with security awareness training.

*Deploy Security Software.* Email filters can help ensure many phishing emails never make it to the inbox of your employees. Next generation endpoint protection can detect and block exploit attempts against client applications and malware from properly executing.

*Patch, patch, patch.* Ensure you are running the current versions of all applications, especially the ubiquitous. Exploits targeting Internet Explorer, Adobe

products and Microsoft Office are common given the fact these applications are so widespread. Ensure your corporate IT department installs patches and updates soon after release (or automatically) as these patches generally fix aspects of the applications that are known to be vulnerable to exploitation.

### Mid-Infection

Once the ransomware has been delivered and executed, it will begin the process of encrypting files in directories to which it has access. This can be particularly devastating if the victim is an individual within a business that maintains significant access to the corporate network such as systems administrators. There have been instances of ransomware encrypting not only the data on the victim machine but also the entire corporate network!

*Control access to corporate data.* Ensure that employees have access only to the portions of the network they need for their specific job function.

*Utilize behavior based attack detection tools.* The RansomWhere? solution referenced above is such a tool. It detects when rapid file creation is occurring in a home directory and immediately halts the process and displays a warning message to the user. The general issue with this approach is false positives- these tools can often block legitimate processes and become a nuisance and present an obstacle to employee efficiency. RansomWhere? attempts to address this through whitelisting known applications and all applications present on the user machine prior to installation. LightCyber and MalwareBytes Anti-Ransomware are other such behavior based detection products. When evaluating such products, read user reviews and beware of false positives.

### Post-Infection

Ransomware has successfully executed on your machine and your data has been encrypted and a ransom demand has been made. Now what?

*Regularly back up your data.* Many businesses have existing data backup policies. Ensure that the data is backed up onto offline systems (i.e. backup and unplug). If the backups are stored to another live system on the network, the cryptor may be able to encrypt your backup files too!

*Investigate the Incident.* Whether you have the capability in house or you need to bring in third party expertise, conduct a robust post mortem investigation of the incident. If you discover, for instance, that you have been hit by something from the TeslaCrypt ransomware family, you're in luck! A master decryption key exists! If the ransomware strain you investigate is either unknown or relatively new, a victim could engage specialized information security services to analyze and reverse engineer the malware to identify any potential vulnerabilities that would allow for a decryption key to be found.

*Pay the ransom?* Most standing guidance from law enforcement and the security community recommends that victims do **not** pay the ransom as this helps perpetuate the success rate of attacks. But as an organization, if you are

There have been instances of ransomware encrypting not only the data on the victim machine but also the entire corporate network!

hit and you have no viable backups and no ability to decrypt the data after your best analysis and reversing efforts, there remains two options: rebuild the lost data from scratch or pay the ransom. If ransom is paid, criminals have been generally reliable in providing the decryption keys.

## Moving Forward

The ease by which cyber criminals can launch ransomware attacks and the lack of an all encompassing defensive solution make it unlikely the prevalence of ransomware will abate anytime soon. An evolution of security solutions towards a unified approach may help organizations better defend themselves by streamlining security deployments. But until researchers (or machines) can figure an efficient way to detect and respond with only a manageable volume of false positives, an enterprise's best defense will continue to be proper data backup practices, sound investment in security product, and employee training and awareness.

**Ryan Lai** has more than10 years experience in the information security industry. His focus area is threat research, and he has substantial experience in business development for the industry in the EMEA and Asia Pacific regions, helping enterprises assess and manage risk across a wide range of business areas. Ryan has a BA in international relations from the University of California, Los Angeles.

# CREATING AN INFOSEC CULTURE

## By Chris Rivinus, Head of IT Finance at Tullow Oil

### Behaviour Is Driven by Emotions

There's an old saying in sales: people don't care how much you know until they know how much you care. But care about what exactly? We've all had the experience of listening to a well-polished sales pitch by an earnest individual who clearly cares about their product or service...but we've been turned off or felt it was a waste of time. A truly compelling sales pitch, one that actually stimulates you to commit spend or to dedicate time and resources, is one that convinces you that the sales person and their team cares about the same things that you consider a priority.

### Organizational Governance Only Goes So Deep

Sales and marketing professionals appreciate the disciplines of sociology, psychology and anthropology and their contribution to our understanding of what drives our decisions at a subconscious level. Our social context and national cultures underpin deep seated feelings that dictate much of our sense of right and wrong and our sense of priorities. And those sensibilities tend to be quite different depending on the communities in which you were raised.

The foundational elements of any individual's inherent values and priorities are cemented well before adulthood. The major influencing elements for shaping those foundations are usually associated with community. It's far more difficult to influence a person's intrinsic sense of right and wrong by mere organizational governance if elements of that governance conflict with the basic cultural values instilled in staff during their childhood.

> The first step is understanding your own cultural biases and how they might differ from those whom you are trying to influence.

That's not to say that organizational governance isn't valuable. To the contrary. It's critical. It tells people what the organization thinks is right and wrong and what the organization's sensibility is around how things should and shouldn't be done in the office. But effective cyber security isn't only about behavior in the office any more. In our always on, everything connected world, what you do at home and online in your personal time, dramatically impacts the susceptibility of your organization.

### The Challenge for Cyber Security in an Always On World

And this leaves cyber security leadership in a bind. How do you create a culture of information security amongst your staff that not only influences behavior in the office, but everywhere else too? I think most people would agree that extending the scope and detail of organizational

> Resistance to policies and behavioural compliance efforts isn't about lazy or deviant behaviour.

governance to dictate behaviour 24x7x365 for all their employees everywhere is not reasonable, nor would it be received favourably if it were even legal.

The first step is understanding your own cultural biases and how they might differ from those whom you are trying to influence. You not only have to show the audience of your security awareness programmes that you care, you have to show them that you care about the same things they care about. If you simply write awareness programme content that you think is compelling to you, you are assuming that the cultural and social values you have held since you were a child are exactly the same as everyone else in the room.

I recently conducted an online survey which received 85 responses from British Nationals who identified themselves as being in 1 of 3 categories:

Non-IT Professional
IT Professional
Information Security/Cyber Security Professional

The survey questions were taken from the work of Dr. Geert Hofstede who has spent his professional career studying the differences between national cultures and has authored several books on organisational culture. Analysis of the survey yields relative scores across 6 dimensions of culture, each of which indicates a particular set of foundational values and life priorities. The results of the study showed a clear and predictable difference in the underlying values held by the 3 different professional demographics.

For instance, Information Security/Cyber Security Professionals scored higher on the *Power Distance Index* (PDI) dimension than IT Professionals and much higher than Non-IT Professionals (see figure 1). Higher scores on this dimension speak to a natural prioritisation of the value for hierarchy, authority and governance more generally. Lower scores speak to a focus on a prioritisation for horizontal collaboration and equality of rights.

For anyone who has been in IT for any amount of time, this isn't really new information. We see this pattern played out time and again in project meetings, requirements gathering sessions and even in security awareness programmes. InfoSec team members champion the merits of control, defense and assurance, whilst the Non-IT Professionals will not prioritise these elements as highly, inherently more likely to favour openness, knowledge sharing and equality of access. What is important for Information Security Professionals to realize is that resistance to their policies and behavioural compliance efforts isn't about lazy or deviant behaviour. It's often about principled resistance along these lines and that resistance may very well not be conscious. It may manifest in an underlying emotion that what is being presented or proposed just "feels wrong."

Similarly, InfoSec professionals scored higher on the dimension of *Assertiveness* (AST) as well. Higher scores here indicate a focus on results and evidence-based logic as the justification for action, authority or change of behaviour. By contrast, lower scores in this dimension are more likely to feel there is more value in collaboration and experimentation even if it leads to failure. My survey results show that Non-IT Professionals are more likely to value the right process being in place over the results that process ultimately produces.

Another notable difference is the scoring around the *Uncertainty Avoidance Index* (UAI) dimension. It's important to understand that this isn't the same as risk avoidance. Higher scores on this dimension indicate an underlying desire for certainty of a result over avoiding a poor result. (An example would be someone who would rather start a fight rather than waiting around to see if the other party will swing first or not.) The scoring in my survey indicates that Information Security Professionals are by and large more comfortable with the unknown. The fairly large differences in scoring between Information Security Professionals and Non-IT Professionals may be why warnings of "possible attacks" are less compelling when intending to use these scenarios to move people emotionally.

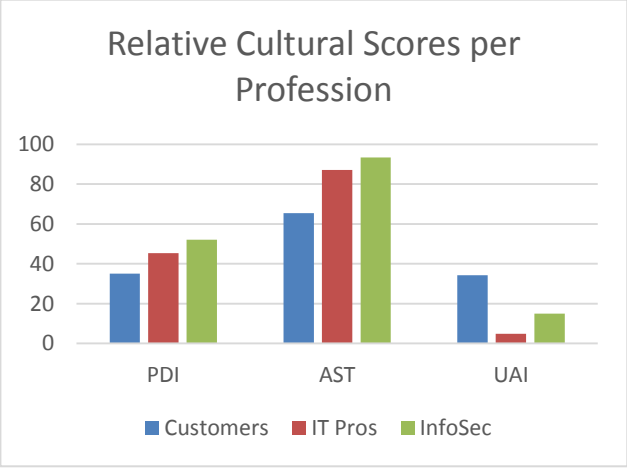



Figure 1 – Survey Results for 3 of Hofstede's 6 Cultural Dimensions.

## So What To Do?

The first thing that Information Security teams need to do is let go of the idea that they need to win the argument. By and large, people are not going to suddenly align their behaviour to cyber security best practices after being shown yet another graph representing another set of statistics or telling the story of yet another breach. There are simply other value systems at play, driving people to care about different priorities. The next generation of cyber security awareness content will ask the question, so what does my audience care about? What are the values driving their priorities? How do I shape my message to appeal to those?

The good news is that the world of marketing and sales have already done much of the heavy lifting on how to answer those types of questions. There are a lot of options out there to help both analyse the underlying cultural values of your intended audiences and shape your content to appeal to those value systems. If you are struggling to understand where to look, drop me a line, I'd be happy to help.

**Chris Rivinus** currently serves as Head of IS Project Delivery for Tullow Oil, plc., and has previously held job titles such as Head of IT Operations, Head of Global Knowledge Management and Head of Global Service Delivery. He holds advanced degrees in cultural anthropology, business administration and international business transactions. His writings on information management, change management and business strategy have been published in research forums, textbooks and mainstream business publications including CIO Magazine, Business Information Review and Knowledge Management Review.
**chris.rivinus@gmail.com**

CYBER
THREAT INTELLIGENCE
& INCIDENT RESPONSE

29-30 November, 2016 | London

# Cyber Threat Intelligence and Incident Response

**Cyber Threat Intelligence and Incident Response**, Cyber IQ's 5th conference of 2016, is the premier forum for cyber security professionals to discuss best practices across both mediums. The event will be hosted in London on the 29th – 30th November 2016.

The challenges of the defender continue to grow as today's adversaries are able to achieve their aims using increasingly advanced tools and techniques designed to circumvent most conventional computer network defense mechanisms, go undetected during the intrusion, and then remain undetected on networks over long periods of time. As such, it is essential for organizations to create effective threat **intelligence and incident response** strategies.

**Cyber threat intelligence** provides network defenders an advantage, using information superiority that can be used to reduce adversary's success ratio. It is an important tool for organizations looking to update their response and detection programs to deal with increasingly sophisticated advanced persistent threats. It is also essential to implement a response plan that aims to manage a cyber security incident in such a way as to limit damage, increase the confidence of external stakeholders, and reduce recovery time and costs.

**Cyber Threat Intelligence and Incident Response** is the **only** conference in Europe that brings together cyber security stake holders and solutions providers from across the industry to gather and discuss the strategic considerations of their information security policy. This event provides an un-missable opportunity to discuss the threats of today and the issues of tomorrow with the most like-minded audience available.

CLICK TO FIND OUT MORE

www.CYBERTHREATEVENT.com

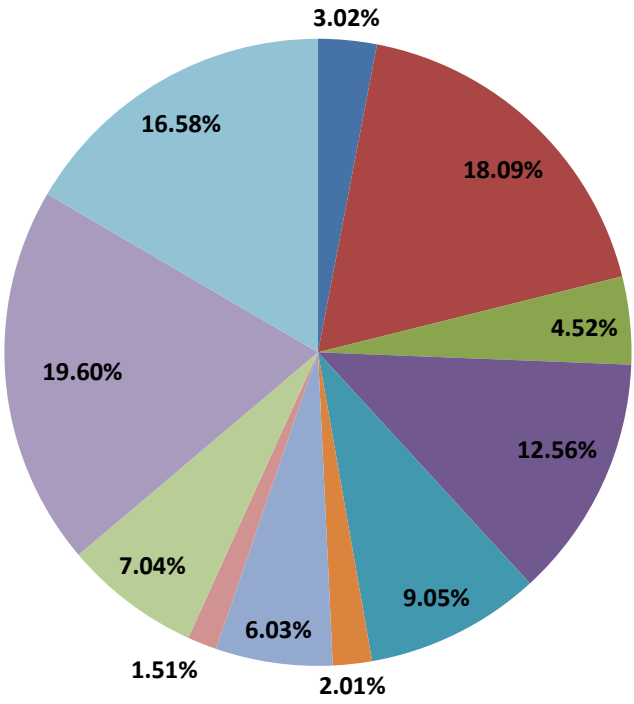
enquire@iqpc.co.uk +44 (0) 207 036 1300

# SUMMER CYBERSECURITY SURVEY

*Insight from hundreds of cyber/Information security professionals*

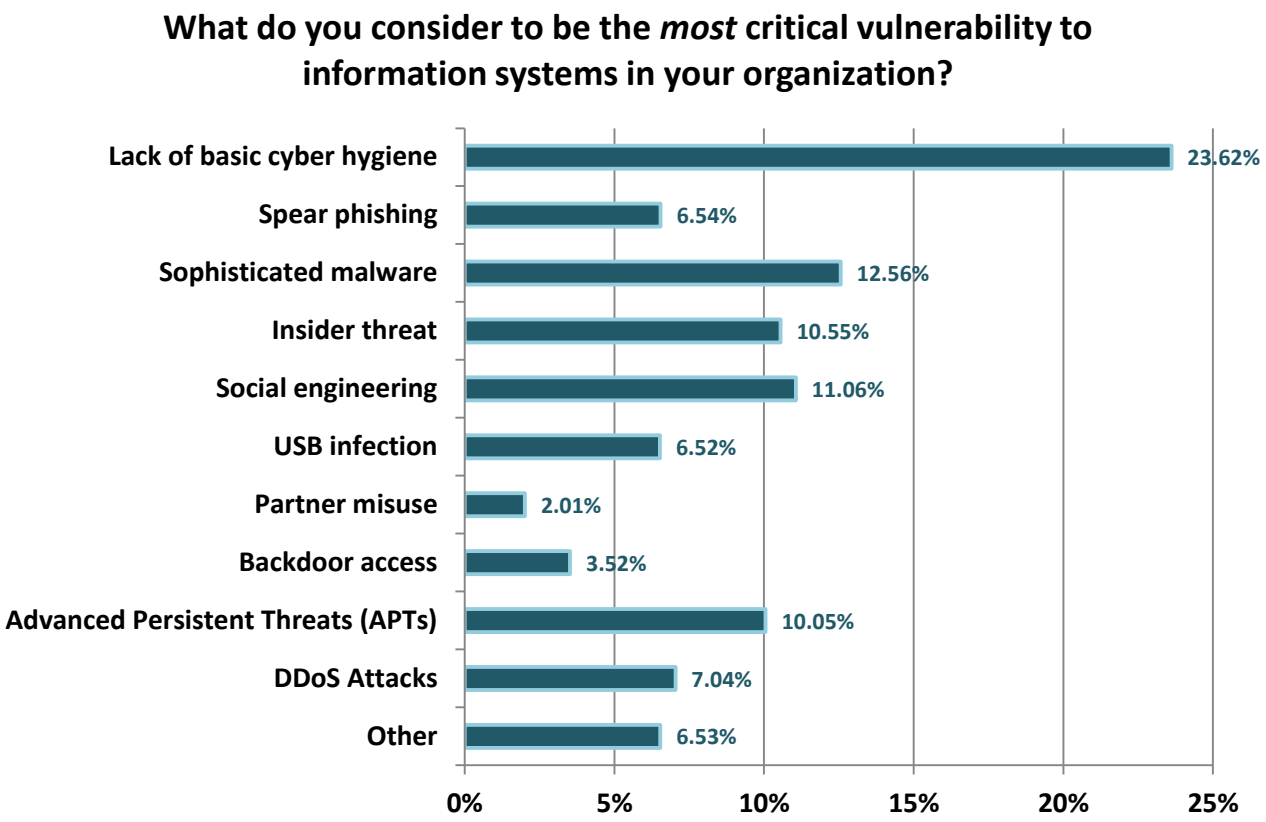
*Cyber IQ*'s summer survey opened the floor to the community in order to discover the general level of confidence when it comes to our readers' own assessments of the level of vulnerability effecting their organizations. We sought to find out the ratio of companies with concrete IT security strategies and provisions to those with limited capabilities or with plans to develop this in the near future. Over 200 international professionals involved in the IT/information security space responded.

**In which sector are you currently employed?**



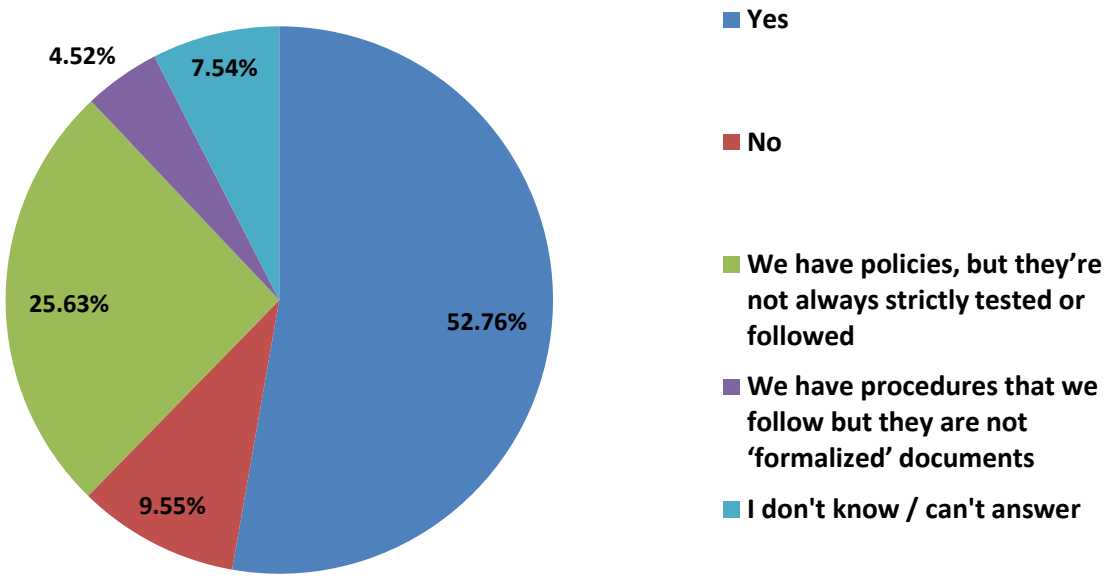

| | |
|---|---|
| Transportation | 3.02% |
| Technology | 18.09% |
| Communications | 4.52% |
| Energy / Utilities | 12.56% |
| Services | 9.05% |
| Consumer Products / Retail | 2.01% |
| Industrial | 6.03% |
| Healthcare | 1.51% |
| Academia / Research | 7.04% |
| Government / Military | 19.60% |
| Other | 16.58% |

The government and military, technology, and energy sectors presented the largest representation among respondents.

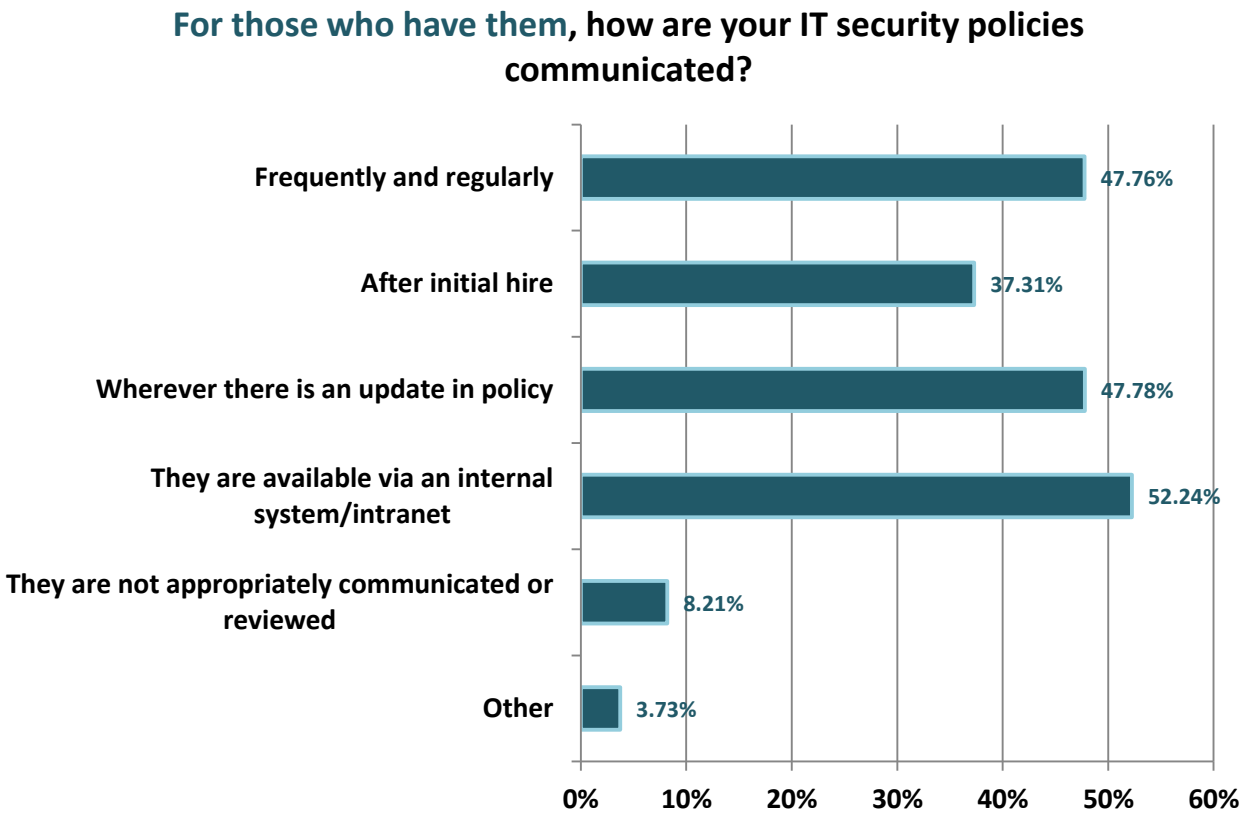



The range of threats facing industries today is broad. Interestingly, almost a quarter of respondents cited a lack of basic cyber hygiene (such as the use of weak passwords and careless talk) was rated as the most critical vulnerability to systems at this time, suggesting that significant improvements can still be made with basic-level education and procedure. However, the rise of sophisticated malware, increasingly savvy social practices and the ever present problem of the insider threat present great anxiety for many. Conventional (and relatively unsophisticated) vulnerabilities that have been known to cause havoc in recent years – including DDoS attacks, spear phishing and USB infection – do not rate highly among the main causes for concern, suggesting that awareness of these issues and the ways to tackle them have perhaps improved.

**When it comes to cybersecurity in your organization, do you have documented IT security policies and procedures in place that are routinely followed and tested?**

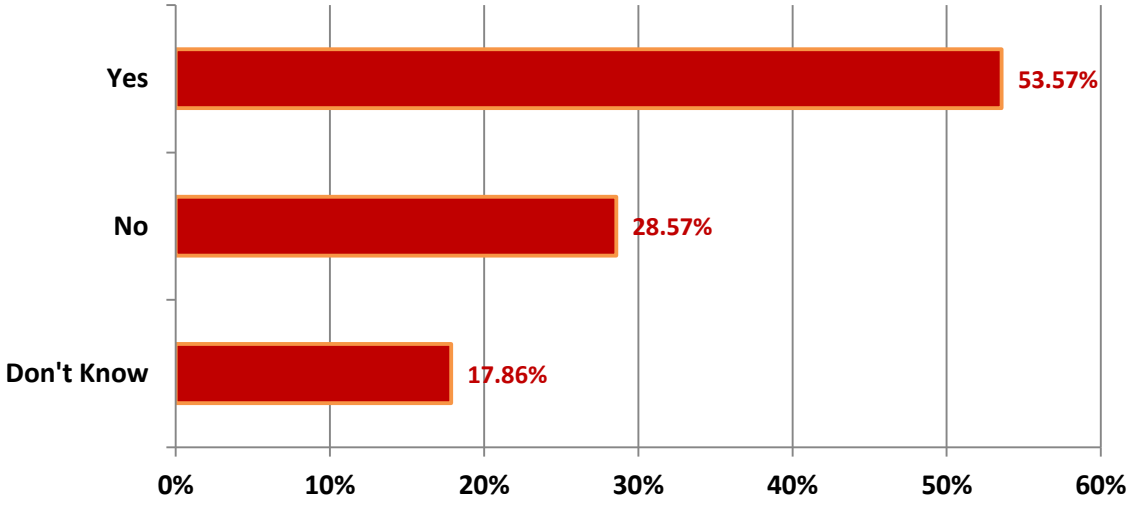



Encouragingly, over half of respondents claim to have a robust policy and procedure process for IT security that is frequently tested and followed, while less than 10 percent admitted to not having these defenses in place. However, more than a quarter of respondents were ready to admit that formal procedures are not always adhered to, suggesting that the human factor – usually as a result of complacency – still presents a major gap in the security chain. This may indicate that organizations need to make more effort to renew and review internal training, and that other means (technology) must be emplaced to reduce the impact of the human gap wherever possible.



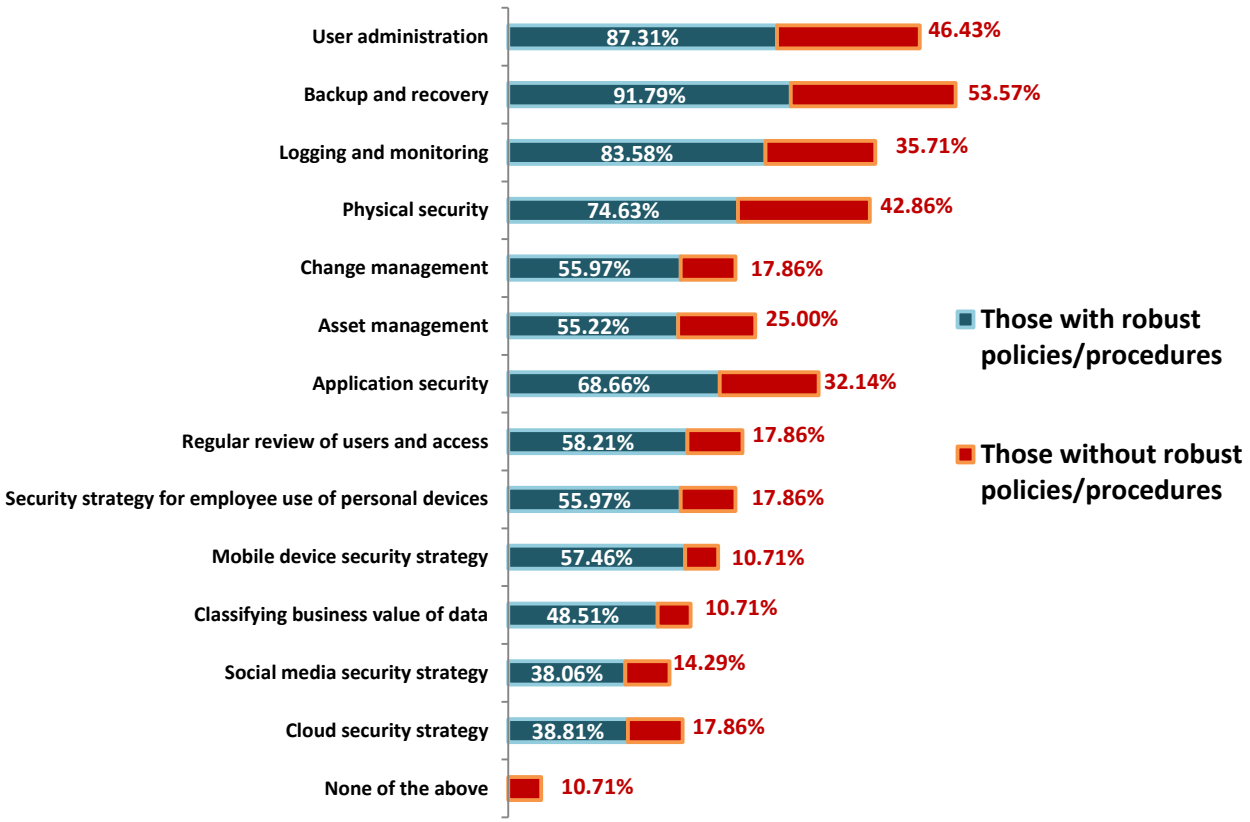

Respondents could select multiple factors. Of those that have IT security policies in place, most see their organizations communicating these through an internal system or intranet. Almost half believe that these policies are communicated frequently, including any time an update is made. However, only 37 percent received a policy document or training session when they were initially hired, a gap that may suggest some staff ignore or do not know the value of security policy updates when it comes to their relevance to the individual employee.

**For those who do not have them, is your organization working on implementing formal IT security policies and procedures within the next year?**

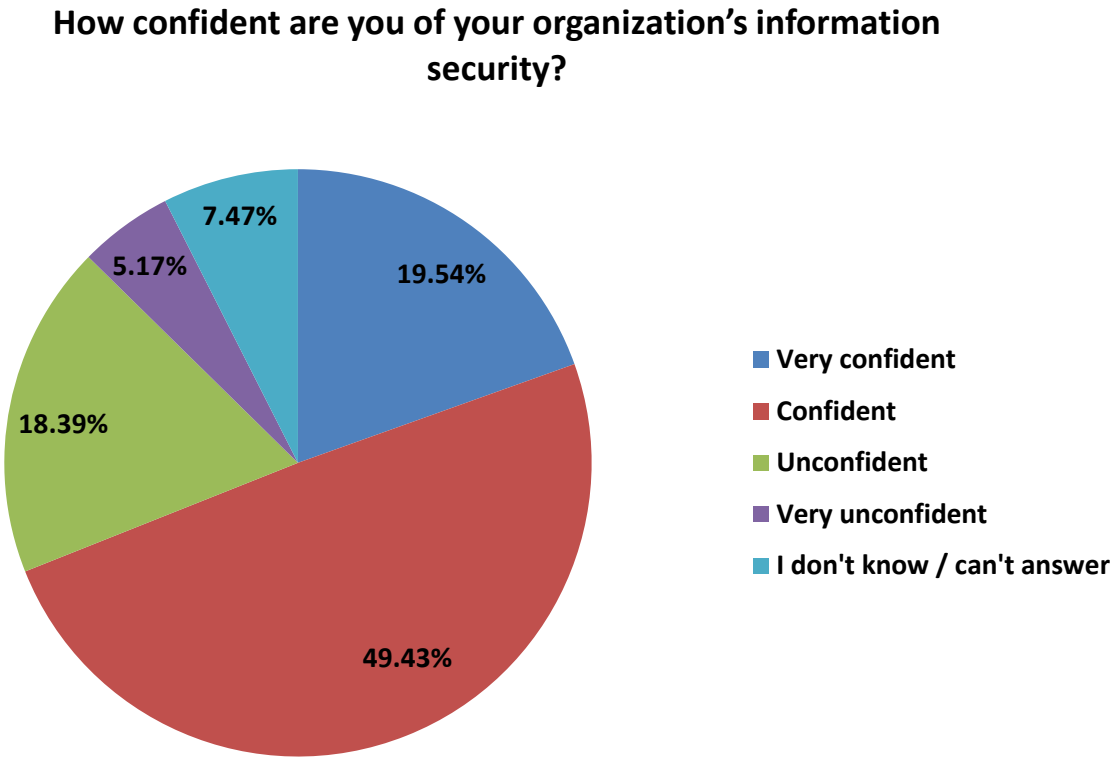



Of those that do not have robust IT security policies and procedures in place, just over half say that their organizations will be working to implement formal changes within the next year to remedy this gap.

## What IT security safeguards does your organization have in place (to your knowledge)?




Respondents could select multiple factors. For both those with and without current policies and procedures governing their IT security, the majority of respondents said they at least had backup and recovery safeguards in place, with user administration and logging and monitoring also on the books. Application security is becoming increasingly more prevalent. A social media strategy was cited as being the least common safeguard of the choices provided. While even those without formalized policies have a breadth of safeguards loosely in place, over 10 percent of them remain almost completely exposed.




Of our 200+ respondents, almost 69 percent said they were confident in their organization's current level of information security, with almost 20 percent claiming to be "very confident". However, this does leave over a fifth of respondents with a clear anxiety over a perceived lack of safeguards in the face of existing and evolving threats. While the results to this question appear to provide a positive outlook, they may also shed light on a dangerous level of over-confidence at large, considering findings from other studies suggesting that the majority of organizations are in fact not prepared for cybersecurity incidents.

# HACKING TEAM FALLOUT:

## *WHO CAN WE TRUST?*

In the summer of 2015, Hacking Team (HT), a well-known cyber intelligence firm, was itself the victim of a cyber attack, losing over 400GB of confidential data that included source code, internal documents and sensitive emails.

Found among the data – which was subsequently dumped online for all to see – were details of the company's customers, a list that included a number of government bodies and law enforcement agencies. Customers included the FBI, DEA, and police forces from Australia to Brazil. Worse still, several entities listed were known to be on blacklists of countries identified as repressive, including Sudan (National Intelligence Security Service) – banned by the UN – and Russia (KVANT, a state-owned military R&D organisation that works with the FSB) – barred by the EU. Also on the list are a number of corporate clients responsible for critical infrastructure, including British Telecom (BT) and Deutsche Bank.

Fallout from the leak has rippled. Of course, no one could have predicted that this firm – let alone any other – would be the subject of such a high-profile scalping. Even so, heads outside of the company have already rolled. In the first instance of an axe dropping, the head of the Cypriot intelligence service was forced to step down after details of the HT tracking system it had employed became public knowledge. Wiretapping equipment doesn't exactly come with the best PR these days.

Not only is the use of HT's surveillance technology controversial, it lost its utility at the point of exposure. If it is known that certain software is being implemented, it can be found. And if it can be found, it can be neutralised. For better or worse, the systems being penetrated by the software – such as iOS, Android and Windows – are being patched to close the zero-day exploits identified through HT's expertise. While this makes life more difficult for many hackers, HT's existing solutions will become redundant, and the company will have to decide whether to start again, fold, rebrand or a combination of the above. On the other side of the coin, hackers have also been analysing the leaked code to find ways to build more robust malware, while less-skilled hackers will be absorbing the HT how-to guides found within the data which had been designed to teach users how to easily employ the tools in question.

David Vincenzetti, HT's CEO, released several statements on the company's website in defense of the company's work. Within one of the more detailed posts, he claimed that HT was in full compliance with the law and had discontinued business with any customer found to be

> Having made a considered judgment on a security investment, that decision has been proved wrong; costing money, capability and reputation.

> Government data could be better secured by enforcing internal policies and scheduling periodic assessment of internal infrastructure and personnel.

using their services for military or unlawful purposes (apparently a violation of its user policy). He also insisted that HT would continue its work within the public security sector:

*"It is the commitment of Hacking Team to develop new and better tools for use by law enforcement. Our software engineers are already at work to create the systems of the future."*

Vincenzetti's reassurances have not placated other companies directly affected by the leak. Netragard, for example, a company that helps customers test their own networks for vulnerabilities, sold a zero-day exploit to HT for a princely sum, only to be exposed by the leak and for the exploit to be rendered useless. Netragard has subsequently apologised for doing business with HT, blaming HT for unethical conduct, and claimed in a blog post that the incident may at least be a positive step for security:

*"HackingTeam is just one example of why the zero-day exploit market needs to be thoughtfully regulated. Regulations should not stifle research nor should they prevent researchers from building zero-day exploits as that would have a profound negative impact on security. Instead, regulations should provide a framework for the legitimate sale of 0-day exploits. They should establish a set of guidelines to help control who can responsibily* [sic] *purchase 0-day exploits. Such regulations would make our jobs as ethical 0-day exploit brokers much easier and far less risky."*

Governments and agencies identified in the leaked data will be nowhere near as positive. They have lost face. Having made a considered judgment on a security investment, that decision has been proved wrong; costing money, capability and reputation. Those clients – as well as all governments, intelligence agencies and law enforcement agencies worldwide – now find themselves in a predicament. Who can they trust? If cybersecurity firms are liable to be attacked in this manner, can any of them be relied to secure sensitive data? Will these entities find themselves having to seek out new solutions every time a firm gets doxxed? Or is this very approach to public-private partnership flawed?

"Considering that potentially every system could be hacked, public as well as private, you cannot underestimate the impact of an attack made by insiders," says Pierluigi Paganini, Chief Information Security Officer of Italy-based security firm Bit4Id.

"It's my opinion that government entities have to use services provided by companies that enforce compliance with principal standards in cyber security. The discussion is more complicated for the Intelligence sector, where contractors must be continuously assessed by government offices and must demonstrate the improvement of the cyber security posture in their organization.

"On the other end, government offices must adopt best practices to ensure that the entire cycle of confidential data management is well managed and secure. This could be achieved by enforcing internal policies and scheduling periodic assessment of internal infrastructure and personnel."

Meanwhile, Stefano Mele, a Milan-based lawyer and member of the Italian Institute of Strategic Studies, told *Defence IQ* that leaks of this type pose significant damage for governments but that blame needs to be appropriately afforded.

"Even if cyber espionage is one of the best and most effective ways to get – both in peacetime and wartime – political, economic and military advantages against enemies and allies, the leaking of these activities adversely influences international relations," said Mele. "The legal ramifications have to be addressed within the criminal law of the state affected by those cyber-espionage activities, not in international law. Therefore, the state must prosecute the subjects that have conducted cyber-espionage activities and not the government that has authorized them."

The trust issue of course pervades other elements of the cyber security domain and severe restrictions, without proper regulation, can result in inverse effects on security. Often this occurs when either the private or public sector fails to understand the situation of the other.

Stuart Edmondson of UK-based Nine23, a mobile technology firm that works with both defence and police forces, explained that the constant fear of losing sensitive data has traditionally held many authorities back from allowing employees the use of standardised software and digital devices. In some instances, agencies have subsequently seen a side effect to these heavy restrictions, with employees using their own devices in an unauthorised fashion.

"[The backlash] to being restricted is down to frustration for the end-user," Edmondson said. "They want flexible systems and SMEs can often provide that better than anyone."

"Even after a company has met the government guidelines, there is the requirement for the company's product to be accredited to ensure it has met the required standards. However, it falls to the user to get this right – they have their own accreditation process; they assess their risk; they have to assure themselves that what they are procuring and sourcing meets the standards. They can't simply pay a company and then wash their hands of responsibility."

> Governments can't simply pay a company and then wash their hands of responsibility.

"On the company side, maintaining credibility and accreditation are of course key, but building a relationship with the customer becomes equally as critical. At Nine23, we're very much focused on the end-user's experience – employing ex-military and ex-police to ensure we fully understand the needs and pressures they face."

Mele also highlighted the significance of the human factor, seeing a need for engagement to extend to the public as much as to companies or governments introducing new cyber solutions.

"People are the backbone of every company, including those who manage sensitive data and hold government accreditation," he said. "We must continue to raise the awareness of the public opinion – at all levels – about cyber-security topics, in order that they clearly understand that cyber-security is a shared responsibility where every single citizen is engaged."

# INTERVIEW: GOVERNMENT-LEVEL CYBERSECURITY AND THE ECONOMY

## *Insight from Baroness Neville-Jones, Former Minister of State for Security and Counter Terrorism*

*Cyber IQ:* **Cyber crime has been estimated to cost the global economy in excess of $400 billion each year. What are the long-term risks to the global (or national) economy and to what extent are state/state-sponsored attacks impacting – if not directly targeting – our economic future?**

*BNJ:* Estimated figures of annual losses to the global economy from cyber crime can run into the trillions, rather than billions, of dollars. The huge variations in estimates show that we do not know what the real figure is, though we can be certain that it is well above the statistics of reported crime. The numbers of known breaches increase every year, implying continuing inadequate data security despite the financial and reputational losses involved. Increased awareness of the risks to company data has still to translate into commensurate action. Cumulatively, theft, including state sponsored theft, of intellectual property is one of the most serious threats to developed economies as it amounts to loss of the seed corn of future prosperity. It takes place in companies of all sizes – smallness is no protection.

**The UK government has been trying to establish resilience in the form of standards and guidelines. However, most of the efforts seem to focus on raising awareness rather than legislating strong security action. Is this a fair assessment? Are private and public entities not already aware enough of the threats – and if so, why are things seemingly at greater risk now than ever?**

Outside regulated sectors of the economy where regulators can, with the cooperation of the companies concerned, lay down resilience requirements and test for their observance – which they are beginning to do (banking is an example) – I doubt that good risk management can be legislated for by the state in respect of cyber security any more than it can or should do for other aspects of corporate management. The government can provide inducements to superior performance which it has been trying to do and a tougher regime of mandatory, public, breach reporting could be instituted. If it ever was, security is no longer a technical matter but a serious and evolving risk for which senior management and board, as custodians of the assets of a company, must take responsibility. The criminals are increasing in sophistication and the data owners are not keeping up.

> Increased awareness of the risks to company data has still to translate into commensurate action.

> Criminals are increasing in sophistication and the data owners are not keeping up.

**During your time as security advisor, where was cyber security investment being focused (e.g. technology; training; etc) and to what extent have things changed today, strategically speaking?**

At government level, the cyber security scene has evolved from basic messaging and guidance about basic issues to putting in place platforms for information sharing with the private sector, developing standards and focussing on national resilience through the development of UK CERT, where there is some way to go to close vulnerability to cyber attack. National rollout of the strategy across companies of all sizes and across regions is needed. Developing the research and skills base of the country remains an urgent priority.

**When it comes to national security, we seem to see the biggest cyber security threats emerging from criminal organizations for monetary gain, and from advanced/persistent attacks by state-run campaigns. On this evidence, is the fear of cyber terrorism or hacktivism overstated? Where should security resources be focused in this domain?**

The day to day threat to this country is criminal, for financial gain. But this does not mean the cyber world cannot be exploited for other purposes – political embarrassment, disruption and the reverse of disruption of systems, taking control of them- an increasing risk as the world of the internet of things approaches. Cyber terrorism is a vague, undefined term. So far there has been no act of terrorism involving loss of life executed by cyber means; terrorists so far preferring kinetic and other methods of death and destruction. But hacktivists show signs of moving on – taking control of autonomous vehicles for instance – and the threat of attacking and/or taking control of networked systems, already practised in a minor way ransom activities, is open to wider groups and their sponsors and could well become a much more significant and extensive threat to national security and the well being of civil society.

**What are you hoping to see from further discussion in this arena?**

I want to hear what [the community] thinks and what worries them. Mine is the need to speed up the effectiveness of our defences against the aspects of cyber attack that we do understand and can defend against if we only gave the matter sufficient priority so that we have energy and resources to focus on the threats down the line where our understanding of how the increase security is low and our defences primitive.

**Rt Hon Baroness Neville-Jones** DCMG, served as Minister of State for Security and Counter Terrorism at the British Home Office and on the National Security Council until standing down to become Special Government Representative to Business for Cyber Security. She was Prime Minister David Cameron's national security adviser while in opposition and authored much of the Conservative party's national security policy.

# CYBER DEFENCE & NETWORK SECURITY

**January, 2017**
**London, United Kingdom**

## The premier cybersecurity symposium incorporating militaries, government and critical national infrastructure at the highest decision making level

As the cyber threat evolves and the incidence of attacks increases, maintaining preparedness and situational awareness is vitally important. Customised malware, DDoS attacks and the vulnerabilities of mobile and enterprise networks all present real challenges. However, the opportunity to come together and share ideas, solutions and initiatives and to facilitate deeper cooperation in cyber defense must be harnessed.

DefenceIQ is delighted to announce the return of our Annual Cyber Defence and Network Security Conference. Building on the success of previous events in the series, our 2017 conference will offer unique accounts of national and corporate cyber defence strategies, including the most recent programmes and requirements, as well as insight into the latest technologies and innovations available from industry. Cyber Defence and Network Security 2017 truly is an unmissable opportunity to learn from international best practice and expand your network of like-minded cyber security professionals.

**Why you should attend Cyber Defence and Network Security 2017:**

- Learn from leading nations on their best cyber security practices, and also the threats that concern them in the future, from best methods of training to concerns around the 'Internet of Things.'
- Improve your knowledge from the industry as to the best tools and solutions available to help ensure total network security.
- Exposure to organizations outside of the military, ranging from private to public services, with the question being posed "What lessons can be learnt from outside of our network?"

**www.CDANS.org**

**enquire@iqpc.co.uk** **+44 (0) 207 036 1300**

# THE 'MR. ROBOT' PROPHECY

## *How likely is it that a cyber attack will cause a global meltdown?*

Last summer saw audiences tuning in to the first season of USA Network's *Mr. Robot*, a show that has since become one of the most-watched new dramas in the U.S. The series follows the life of an alienated young hacker who becomes involved in a plot to bring down the global economy with a coordinated cyber attack, motivating mass debt cancellation and the rebalancing of wealth. Rallying against the glut of previous onscreen techno-thrillers, the producers have aimed to portray hacking in a more realistic light (strictly no 3D wireframe cities or *Tron*-esque circuit board battles). The question is, just how realistic is this fragile tele-world?

When it comes to foreshadowing, *Mr. Robot* has already nailed a few eerie similarities to recent events IRL. An Ashley Madison-style data dump provided a plot point for the writers long-before the real dump occurred in August 2015. References to an economic collapse in Europe spurred by a Chinese stock market implosion skirted uncomfortably close to the recent 'Black Monday' slide, which some feared was about to ring in a new global recession. Another scene in the last episode – though entirely unrelated to hacking – was also near enough to the reality of the Virginia/WDBJ shootings that airing of the episode had to be postponed.

Meanwhile, the series manages to make gripping viewing out of relatively humdrum moments of coding. A RUDY attack becomes a nail-biting race to shut

down a CS30 server. A RAT (Remote Access Trojan) is employed and leads to the breakdown of a relationship. An Android phone is infected with a monitoring tool for nefarious purposes. These incidents further draw attention to the idea that cyber attacks, while potentially devastating, ultimately come down to two grey factors: engineering skill and time.

Today, many of the world's internet users possess an abundance of both. But with 'script kiddies' able to simply download pre-programmed tools and execute them with little effort, neither factor is even much of a hurdle when it comes to disrupting systems at a base level. The most damning notion the show highlights is that even the biggest corporations and the most advanced cybersecurity firms are deeply vulnerable to being taken down by a single intrusion.

For 'Evil Corp' (itself modelled on an unflattering mashup of Enron and other multinationals), read Sony or JP Morgan Chase. Both suffered high-profile data breaches within the past year. The misfortunes of 'AllSafe' – the show's cyber firm – are not a million miles from the calamity experienced last year by Milan-based Hacking Team. Meanwhile, there's barely a mask between the fictional FSociety and the real-life Anonymous, or the ill-fated 'Omegas' and the real-life Lulzsec.

So with this dark mirror in mind, how likely is it that a coordinated cyber attack will collapse the global economy?

Most governments at least believe that the general threat of cyber criminality is worth heavy investment, proving that there at least remains a gap to close – and to continue to close – as threats become more numerous and sophisticated. The problems arise more in the corporate world. The majority of businesses are simply not prepared. This is a cold truth commonly verified by analysts from both the private and public sectors, and remains the number one weak link in the chain when it comes to national security. The portrayal of a world that overestimates its own security – and thereby underestimates the most severe possibilities – does appear to correlate.

That brings us to the capabilities portrayed in the show. The hacktivists in *Mr. Robot* are smart and opportunistic but the schemes often rely on luck and circumstance. Okay – this may be partly designed to create a more dramatic story, but the steps the TV show treads are not far off when we consider the series of events needed for a real world hacker to slip through a net – namely the concepts of employee incompetence and the insider threat. This includes scenes featuring a naïve CTO who places too much trust in his more capable engineers and an inept security guard who runs an open-source fact-check to verify the suitability of a person trying to enter a server facility. This human factor is a real problem. In fact, it is statistically the biggest problem. IBM pins 95 percent of cybersecurity flaws on human error. Initiatives like the UK's new *Cyber Essentials* scheme are trying to tackle this by ensuring companies undertake basic hygiene procedures and educating the average worker to avoid simple pitfalls, but it is not a problem that can be solved overnight.

> Even the biggest corporations and the most advanced cybersecurity firms are vulnerable to being taken down.

The insider threat is arguably a more 'lethal' human hazard. In the show, FSociety's entire plan hinges on the use of an insider – our protagonist – as well as the decisions of others 'behind enemy lines' to overlook the criminal activity taking place. In the real world, work is being undertaken to not only enhance the monitoring of employee activity but to pre-emptively pinpoint where disgruntled staff are most likely to pose a threat by monitoring patterns of behaviour. Several academic projects are experimenting with algorithms for this very purpose. Software that flags possible rogue employees is still a fledgling technology, but it is now considered viable enough to be trialled in the workplace.

As with any criminal activity, we must not only consider the opportunity but also the motive. State-on-state cyber attacks are already known to have an economic impact – particularly when it comes to the theft of intellectual property – but the likelihood of a nation attempting to

demolish another at its financial foundations seems slender. We've already mentioned the integration of the global economy and the domino effect that can occur when one market falls. As such, it would seem foolhardy for any country to consider an 'economic strike' unless it is sufficiently independent and sheltered from the collateral. At the same time, it would need to ensure its allies were equally safe from the blowback. Currently, there are few countries – if any – that could claim that sort of economic detachment. State attacks have been known to disrupt critical infrastructure, but most of these have had a relatively contained effect and have comprised only a part of a wider strategic operation (such as the 2008 Russian invasion of Georgia). However, others disagree with this conclusion, citing evidence in the fact that some nations are now beginning to hedge themselves off.

"The international payment clearance system (SWIFT) is a prime target," says Bob Marshall, a former systems engineer with MITRE Corporation.

"Hundreds of billions of dollars a day flow through it. If there is one place where the world has a single point of failure, this is it. International finance would come to a complete halt if it went down. It is a decades old system and is used by thousands of financial entities meaning there are many entry points.

"Who would want to harm it? Certainly a country that has been prevented from using it would have a motive. Some people have suggested that Russia be banned. I feel that would be an extremely dangerous thing to do. The chaos that would result from this antiquated system's collapse would have enormous effects on the world's economy."

To provide further scope, last year saw the establishment of China's own, alternative international payment system (CIPS) which serves to process *cross-border yuan transactions* and may be launched as early as September or October. Meanwhile, Russia's Central Bank announced last December that it had launched a domestic rival to SWIFT with over 90 banks involved. The BRICS nations are also consulting on an alternative to SWIFT to "protect the member countries from any possible disruptions and provide better security."

*Enex TestLab* published a theory in June that existing and former communist countries are being incentivised to hack western organisations on a platform of wealth redistribution:

*"The nations that were staunch proponents of communism throughout these eras, such as Russia and China, are trying to make up for lost time. Money is the universal language, but they have 40+ years to make up for. How does one accumulate wealth at an accelerated rate to make up for lost time in the information age? If the stats are anything to go by, cyber-attacks, fraud and hacking are a safe bet. With 45% of the world's hackers coming out of China and Russia, it seems to be paying off."*

Beyond state activity, attacks undertaken by criminal organisations and opportunists – which consistently accounts for the majority of day-to-day cyber incidents – are most commonly rooted in monetary gain. It's true that these crimes have a damaging effect on the economy – around $445 billion a year. The question then becomes, why topple a market when you can steal money with relative ease and then benefit from the system you inhabit?

Of course, *Mr. Robot*'s antagonists are ideologically motivated, seeing themselves not as profiteers but as freedom fighters. The question is, would any of the usual suspects legitimately wish to crash the world's markets? Real life hacktivist groups have been largely limited to attacking single entities and organisations to prove

a point, be it the defacing of a website as a warning shot to a rival 'clan' or mass data leaking to undermine public confidence. Even the Sony hack, suggested to be the result of a state-sponsored use of hackers, or a hacktivist group aided by a disgruntled insider, sought *extortion* as its objective – not the collapse of Sony (at least as far as we know). Likewise, no true cyber-terrorist group has yet caused the so-called 'Cyber 9/11' that is predicted year on year, nor is there ample evidence that terrorists would prefer to undertake this route than more lethal, 'kinetic' activities. Should this happen, analysts are wagering more on the disruption of power or communication networks rather than of direct attacks on the economy. After all, many people do not bat an eyelid when share prices fall, but almost everyone is disturbed by suicide bombs or shootings.

All that said, there is evidence that motive is redundant. The University of Cambridge Centre for Risk Studies has evaluated a hypothetical scenario in which a power grid failure can cost the United States more than $1 trillion, owing to damage of infrastructure and business supply chains. The insurance industry alone would be expected to lose up to $70 billion. In such a case (although described as "not likely to occur" by the study findings), mass damage to the global economy could be obtained, on few resources, without first having an intention of collapsing the world's markets.

Advanced state hackers or terrorists may even see this as a preferable tactic to attempting a full-scale cyber onslaught, seeding only a few necessary interruptions needed to trigger a cascade.

TV drama shows may often play fast and loose when it comes to authenticity but in their ability to simulate possible outcomes (and often the *worst* possible outcomes), decision-makers should view them as a chance to absorb free lessons – before reality catches up.

A power grid failure can cost the United States more than $1 trillion, owing to damage of infrastructure and business supply chains.

# THE PERFECT PR PLAYBOOK

## *Saving the reputation of your business after a cyber attack*

Continuing escalation in both the frequency and severity of cyber attacks on commercial companies suggests there is now a clear threat to all businesses and customers. While the problem is recognized among most large-scale enterprises (i.e. those with the capital to invest in high-end cybersecurity), there remains an inability for any network to remain 100 percent secure. This means that, for now, the average likelihood of a data breach remains high across the spectrum while the capacity for prevention is worryingly outpaced by the capacity of the threat.

This is not to say that small businesses are at less risk. Proportionately speaking, the opposite has been true. U.S. Government analysis back in 2010 found that more than 60 percent of businesses targeted were those with fewer than 100 employees. Further studies indicated that 20 percent of small businesses were attacked every year, of which 60 percent declared closure within the following six months. In 2012, the UK's Department for Business, Innovation and Skills found that 93 percent of large businesses reported a cyber attack, compared to 87 percent of small and mid-size businesses. While this may represent a shift towards hackers targeting bigger fish, it is worth bearing in mind that many small businesses are never aware of the attacks taking place on their networks, while larger enterprises will have enhanced ability to monitor these attempts. Also keep in mind that businesses are not obligated to report an attack.

Increasingly, cases involving large enterprises have seen cyber criminals not directly targeting the company's accounts, but instead aiming for the private data belonging to their customers. Be it credit card details or personal identity information, the motivation for attack can lie anywhere from illegal profit to deliberate attempts to damage a business's reputation. Some are even undertaken solely for bragging rights.

Given this high-risk, low-prevention scenario, all customer-oriented companies must therefore prepare to deal with the aftermath of a cyber incident. However, because of the mantra of cybersecurity experts that demands a focus on "prevention not reaction", many companies fail to place enough investment into reaction whatsoever. A 2013 survey conducted by Ernst & Young found that 96 percent of executives don't believe their business is prepared to handle a cyber attack.

> 96 percent of executives don't believe their business is prepared to handle a cyber attack.

## Risking Reputation

According to management consultancy Reputation Institute, a 'reputation' is the emotional connection stakeholders have with a company. Disclosure of data breaches is said to break the emotional connection – or trust – between the company and its stakeholders. In this age of information, a torrent of media and social media attention piles negative perception onto the business in terms of its competency, where often the leak of customer information is conflated with a perception of negligence towards the customer. This can occur in spite of the many measures taken to avoid these incidents. When it comes to commerce, companies are rarely treated with the sympathy that individual victims of cyber attacks receive, meaning that many customers will commonly feel the company is as much to blame as the perpetrator – without necessarily knowing the root causes.

This perception has been supported by various studies. In one 2014 U.S.-based survey, the Ponemon Institute ('The Aftermath of a Mega Data Breach: Consumer Sentiment') found that 67 percent of consumers felt that a company should be obligated to financially compensate them in the event of a data breach, with around 60 percent expecting complimentary identity theft protection and credit-monitoring services. The same study indicated that 76 percent of U.S. customers described their response to a data breach as "stressful", with 25 percent experiencing fraudulent charges on their credit cards. 29 percent of existing customers would subsequently be less likely to continue a relationship with a company. This last figure is of particular interest. It suggests that most customers are forgiving, or at least understand that the risk of providing their data is worthwhile if indeed the product or service is satisfactory. This is understandable given that notifications of data breaches are so common in this day and age. Moreover, the figure suggests that at least some of the fraction of customers wary of continuing a relationship with the business are still open to being won back. That process of course begins with a strong public relations campaign.

## Building Back Trust

Foremost, a quick and clinical public response is a must. There should not be a drawn-out debate over whether to disclose the breach – that decision should already have been determined by the company's incident response strategy. Delaying disclosure makes the problem worse by leaving customers' data vulnerable for longer, preventing them from making card cancellations or password changes when they may be at most risk. Delay also runs the risk that the media picks up on the story before the company has the chance to notify the public and 'own the narrative'. Trust requires immediate honesty and confident guidance from the company as to the recommended course of action.
Direct communication can make a vast difference to consumers at a time when anxiety is at its peak. Companies should be prepared to notify their customers by email (and by letter in more serious cases, such as in banking incidents). Customers should be made aware of how

to reach the company for more information and a dedicated campaign should be enacted by the customer service team to address each individual query without delay.

Other stakeholders, such as investors, may be more concerned with the press fallout impacting stock prices and valuation. Companies should supply information on how it is acting to restore and recover its customers' business and the reputation of its brand. Openness must also be offered when it comes to communicating with regulators and authorities. Ultimately, while the official notification must remain consistent, it must also be tailored depending on the specific audience for which it is intended.

## Taking Control of the Media Response

After disclosure, public panic will take to the press and to social media. Companies can neither ignore this conversation nor try to shut it down. Instead, they must contribute to it and ensure that all official accounts (such as Twitter, Facebook and the corporate website) provide an official statement, immediate guidelines for action, contact details for customer and press information, and regular updates on the process of restoration. This way, an explosion of false rumors can be minimized. In some incidents, secondary groups of criminal opportunists have used this moment of uncertainty to capture further data because companies have not made it clear where official information can be found.

In all situations, apology should be policy, regardless of how the breach occurred. That apology should be clearly delivered within the context of how the company is rectifying the situation. Scripted responses should also be prepared for spokespeople to adhere to when fielding questions from the press or from investors and customers.

## Bringing in Outside Help

If a company has determined that it cannot cope with managing its own crisis response, private PR firms may be the answer. Some now specialize in damage control for exactly these scenarios. Knowing which firms can live up to their promises, having them understand the nuances of an individual business, assessing their full costs, and having them readied on speed-dial is all best established before a crisis occurs. Likewise, it is essential that insurance policies and legal standing are also reviewed in detail to account for 'cyber liability'.

## Offering New Services

Placating the customer can be an easier process if other forms of compensation are offered, such as complimentary services that demonstrate action against repeat incidents. As in the case of Target (2013), free credit monitoring was offered to all effected shoppers alongside the CEO's email notification and apology. Other tokens of good will may include discounts and gift cards which can of course only be used if the customer remains with the business. Many of these services may come at a cost, but on balance, could prove less expensive than losing anxious people in the long-term.

## Identifying the Mutual Threat

Attribution of a cyber attack is notoriously difficult to determine. However, in many cases of enterprise data breaches, hacking groups flag their involvement or authorities eventually trace the perpetrator. Helping to establish the source of an attack and stressing the seriousness of the situation will help the public identify a mutual threat and more readily accept an 'all in this together' stance.

# INDUSTRIAL OT-IT CONVERGENCE

## *Is it really inevitable?*

At last year's Cyber Security for ICS Europe conference, one of the liveliest topics of discussion considered the widespread segregation of IT (information technology) and OT (operational technology) departments, and the prospects for convergence.

Traditional management of both sides is now appearing to be outdated, as IT is no longer restricted to back-office business and OT is no longer living in a bubble of SCADA and distribution management systems. The velocity of change in the technological environment has been pushing the two 'sides' together, and most importantly, the threats emerging in the cyber security space are forcing them to collaborate with increasing urgency.

However, change cannot happen solely from an organic perspective. Organisations must implement change, sign off on restructuring, investment, resources and a plethora of other factors that can make the difference between a successful convergence and a failed attempt at one. Doing this can not only be expensive, but culturally daunting. Many organisations have become so set in their ways that the prospect of restructuring is now the elephant in the room. Where do you start? How much will it cost? What skills do you need, and how do you blend them? Will legacy systems need a complete overhaul? Who will be accountable for vulnerabilities? How long will it take for the new team to 'settle in'?...

As the list of questions grows, many experts involved in ICS are doing what they can to guide others towards convergence before the risks become overwhelming.

"There appear to be some cultural differences between the control engineers and the security engineers," says Professor Chris Hankin, director of the Institute for Security Science and Technology at Imperial College. "The former have greater concerns about safety than security. There needs to be an understanding that a system cannot be safe if it is not also secure — emerging standards are beginning to recognise this and this will hopefully lead to some rapprochement between the two cultures."

Eirann Leverett, senior risk researcher at the Cambridge Centre for Risk Studies, agrees. "This problem is primarily cultural but it is possible to bridge such a gap if team members are chosen to work together carefully," he says. "It takes a year or two to 'convert' such mind-sets into protecting the process. Both sides

have valid views, but they each need to understand the limits of their own knowledge, which sometimes limit their responses to a problem. An IT support person might try to protect the data out of habit and violate a safety limit, which is inappropriate in this environment. An engineer however, might never realise how useful a cryptographic signing of firmware can increase confidence that assets have not been altered, and thus increase lock-out-tag-out safety."

Accepting the problem is one thing, but providing a strategic model to making binding the IT-OT parties are also being offered. David Willacy, strategy and planning manager at National Grid, suggests reshuffling the cards.

"From my point of view, within IT security, we've always got this 'CIA' mentality – confidentiality, integrity, availability," Willacy explains. "For process control, it's usually 'AIC'. But as far as the OT and IT departments are concerned, CIA *should* mean cooperation, integration and alignment. We need to have that overlap. We need IT skills within the operational field, and we need the operational skills and knowledge within IT security. That relationship really needs to be created now. I think the best thing to do with security is to move it out of IS (information services) on its own so that it's not seen as part of the IS dept, but as a separate body that can bridge the IT-OT gap."

One major difference lies in the fact that the OT arena tends to be built around small teams diversely located around multiple assets, while IT tends to exist as a centralised team within a corporate business.

On top of this, the environment has changed dramatically. Networks and systems have become vastly more complex. 20 years ago, an OT system may have had 50 configuration settings. Ten years ago, that same system could have grown to 500. Today, it could be as much as 250,000. Disaster can strike if just one of those configurations goes wrong.

The result is that skillsets are becoming wider even though most teams are not getting bigger. There remains the same level of resource. Despite the use of standard IT components making systems cheaper to buy and install, the requirements for the engineers have exploded to the point where the same team of process control engineers now need to be experts in IT, security, virtualisation, and more.

William Horner, an independent process automation consultant who has worked in security for fourteen years, does not believe it is practical to build a team for every asset and expect to cover all the skills needed to cover the broadening types of threat in the cyber security world.

"I get incredibly worried when I see 'us and them' relationships in the approach and technology," he admits. "For me, that's just an invitation for someone to spot the weakness. If there's a gap in the middle, someone is going to walk through it."

"The name of the game is looking at the team, at the skills we now require, and knowing where we're going to get access to those skills. It's not necessarily vendors, it's not necessarily services, it's knowing who has the skills and where they are going to come from. In my experience, it takes about 18 months to two years to train an IT person for OT to a point where they can be autonomous.

> There needs to be an understanding that a system cannot be safe if it is not also secure.

Meanwhile, not all are convinced convergence is the best approach at this time –at least, not for everyone. Martin Visser, security officer process automation at Amsterdam-based Waternet, has over 35 years of experience in the ICS environment. While he believes it is important to centre the convergence around people that have the right knowledge and experience, he has seen limitations when it comes to doing this at a practical level.

"Yes, you can combine them, as smaller companies in the Netherlands have," he says, "but it works but only to SCADA level. After that, in control level, a combination of OT-IT often proves to be a problem. Those worlds often don't understand each other. So many organisations have to think about whether they can afford to invest in a separate OT and IT dept. Depending on the size of the company, I actually think it's worthwhile investing in separation."

"What I see is that when we look to resource the right skills, an OT guy with a lot of experience and knowledge can easily switch over to IT, but an IT guy will find it much more difficult to go the other way. That has to do with the structure of the current organisational environment."

Whatever the recommended models, the undeniable fact on which everyone can agree is that security does not recognise organisational boundaries. Approaches will vary, but the bottom line remains the same. Formulating a way to protect that bottom line must begin now.

20 years ago, an OT system may have had 50 configuration settings. Today, it could be as much as 250,000.

# DACH ICS CYBER SECURITY

BOOK TODAY

**12 - 14 September, 2016**
**Dortmund, Germany**

**On July 25, 2015, the long awaited and controversially discussed IT-Security Act (ITSA) came into force.**

The 2014 hack attack which caused 'massive damage' at a German steel mill highlighted the vulnerabilities faced within manufacturing and industry.
As one of the only attacks on industrial systems to cause damage, the industrial world's eyes were opened to the need for secure Industrial Control Systems to prevent malicious attacks.

The IT SA highlights the seven key areas of critical national infrastructure, and the enforcement of regulatory measures, with fines upwards of 50,000 Euros being threatened if basic standards are not met within 2 years, the need to understand these regulations and best practices to protect against intrusions is more prevalent than ever. Of the key areas mentioned in the act, the Transport, Water Telecommunications and Energy sectors show the importance that ICS Security will play in this standardization process.

**Cyber Security for ICS, DACH 12th - 14th September 2016 is the must attend event in the DACH region that will continue the tradition of the 3 successful ICS conferences in London, uniting both Control Systems Managers with Cyber Security Managers to continue to address the key challenges that both parties face when securing their industrial control systems.**

**WWW.ICSCYBERSECURITYDACH.COM**

**enquire@iqpc.co.uk** **+44 (0) 207 036 1300**

# INTERVIEW: CYBER RISK FOR FINANCIAL SERVICES

## *Insight from Dr. Peter Mitic, Head of Operational Risk Methodology UK, Banco Santander*

*Disclaimer: The individual views and opinions expressed in this article do not necessarily represent those of Cyber IQ or any other organization.*

**Peter, are the efforts being made to introduce information security risk measures in the financial services sector making a positive difference?**

Yes, they are. However, there is always a balance to be struck between making transactions and data secure and a 'nuisance factor' for customers. Security measures may annoy people, so they need to be minimal, but effective. Added to that, it costs time and money to put security measures in place. Fraud analysts at a bank I worked for a few years ago say they can determine the extent of their future external fraud losses by 'tuning' their security measures. They were losing customers as a result of tightening security. Increasing or decreasing the amount of fraud is always at the expense of the nuisance value to customers and to the organisation itself.

We've lost the simplicity we used to enjoy when going to a branch. You could go to the counter, and you would probably be known there. Security was not a problem. When ATMs became available, it was very convenient for customers because they were not restricted to opening hours. However, you need a PIN to use a card in an ATM, and you need to remember it and keep it secret. Maybe that's less of a nuisance than having to go into a branch, but it is certainly more than a nuisance if there is an instance of card fraud.

Now that we have the internet, it's even more convenient for customers, but transactions are much more subject to fraud. Anti-fraud measures are in place, but we are still dependent on passwords

> Santander is changing its approach to try to better manage and mitigate risk by introducing voice recognition.

> The training process is rather like book learning for an exam. It's easily forgotten.

and PINs. I think we need to find alternative ways of identification. That's underway at Santander and also at other banks.

**So it's not the case that today's customers are expecting tighter security processes as par for the course, and always prefer security over ease of use? They are still seeking the easier options?**

People want ease of use and watertight security. The problem is that they don't always go together. Customers want their money to be safe, and to be able to access it without too much of a fuss. Financial institutions want the same.

**Is this model of trying to balance security and 'nuisance' measures something other services are applying as the general standard? Is there another way of doing it? Because it seems less than perfect...**

There are other ways. Santander is changing its approach to try to better manage and mitigate risk. It seems to me that if you know a password, and maybe one or two personal details as well, you can still access an account, no matter who you are. The bank can't see you. I've been arguing for some time that we need to scrap the whole concept of passwords and PINs completely. People forget passwords, and passwords can be compromised too easily. Some time ago I suggested replacing passwords with facial recognition, which requires new software and hardware. In particular, it needs a separate physical device. That would be rather harder to hack.

What Santander have actually settled on – and I think they must have decided on this some time ago – is voice recognition. We started a project where we will, indeed, abandon passwords. There are precedents for using a voice print. Some of the 'challenger' banks have no or few branches. They rely on online transactions, so it's vital that they make the process as secure as possible, and voice recognition is a prime candidate as a means of identification. HMRC has already taken the same approach. Using voice recognition, or anything like it, is not without its problems. We do not want genuine customers to be rejected because, for whatever reason, their voice is not recognised as genuine. We'll be testing the system rigorously to make sure that doesn't happen.

**Let's talk training and education. What does the overall concept of cyber risk mean for staff and their training, or indeed, the education of the customer base. Do you think that's evolving?**

In common with other banks, we tell our customers that they must ensure their own security by, for example, not divulging their PIN or password, using virus protection software and not responding to suspicious emails. That's a fundamental change from the time before internet use became widespread. Then, the bank was solely responsible for the safekeeping of your money. Now, you are too. It's an important point that is often overlooked. There is no guarantee that customer education works. People don't always do as they should, and they simply make mistakes.

As part of our internal training we cover what the security measures are, and what to do if we suspect that activities such as money laundering and fraud have occurred. It's the same at all financial institutions. Many staff don't have direct experience of the issues covered, so the training process is rather like book learning for an exam. It's easily forgotten.

**Presumably, the rate of the training is not necessarily consistent, frequent, updated...**

It has to be done every year, and it does get updated every year, particularly in the light of new legislation. That's not the problem. It's tempting to regard it as a lower priority than other work that has a hard deadline.

**Is this just symptomatic of office culture? We've heard from others in the cyber security field that senior management also responds poorly when they are told of the negatives – how they're 'losing' – and that if we reframe the discussion to show them how to 'win', they are more likely to get on board. Do you think that could be at the root of the problem?**

I suspect not, at least as far as people who work in the banks are concerned. Many of them have no direct involvement with cyber crime. Our senior staff are very aware that we can 'win' by mitigating losses. That's integral in the training.

The other side of it is what the customer sees. I've already mentioned that despite 'education', customers are still caught out. Many customers find that the measures that we say they should use to protect themselves against cyber crime are just not practical. For example, it's difficult to remember multiple passwords, so they either use one only, or write them all down. Neither is recommended.

**Knowing how your immediate staff are engaging with information security is one thing, but when you're working with third party suppliers, you can't always manage or control what they're doing or the level of intellect they're bringing to the table. How much of a risk lies there?**

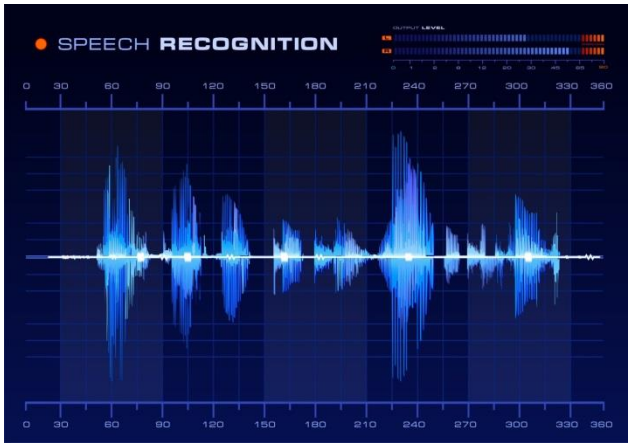
You would have to make sure that you take the same approach that you would when you buy insurance. Liability is passed down the line. So your third party supplier would be responsible for anything that goes wrong.

It doesn't quite work like that in some aspects of banking. With regulatory restrictions, for example, you are responsible for any fault of any third party equipment or procedure. You have to make sure that they're at the right standard, and that puts the banks in a very awkward position. If a bank buys software, the seller of that software might retain intellectual property rights over the software. If it's an algorithm, for example, they possibly won't even divulge what it is. We have that issue with some of our software, and I've seen the same thing in other organisations. We have to guarantee that what we bought works, even though we don't know what it is. So if it doesn't work as it should, we're in trouble. That's where our risk lies.

**It comes back to security versus nuisance. It's a necessary evil.**

Yes.

> We have to guarantee that what we bought works, even though we don't know what it is.




**You'll be speaking just as frankly at October's Information Security for Financial Services conference. Is there anything that's proving of particular significance to our audience this year?**

Aside to mentioning that both the bank and the customer are jointly responsible for the safekeeping of customer accounts, there is an issue which I imagine many people are not aware of – and it's a legal point. It's a question of who is liable, in the event of a security breach or a fraud. In a physical robbery, money is stolen from the bank as a whole, not from an individual account. With cyber crime it's the other way around. A loss is suffered by an individual customer: it is not shared among all customers.

Physical crime has decreased markedly over the years to almost nothing. The reason is that we have improved security measures to the extent that physical theft becomes almost impossible. A rough calculation indicates that if you want to make a living out of robbing banks, your expected income is about £30,000 a year. It's tax free, which is very nice, it's not brilliant!

In parallel with declining physical crime, cyber crime is increasing markedly. Physical crime involving coercion (i.e. 'robbery') is more serious then cyber crime, which is classified as 'theft'. The maximum penalty for robbery is 'life', whereas the maximum penalty for theft is ten years behind bars. Meanwhile, the chances of apprehending and convicting a cyber criminal are much less than apprehending and convicting a bank robber. I think that cyber crime and robbery should carry the same status in law.

The problem for the customer is then that the bank may not reimburse the loss.

> Cyber crime and robbery should carry the same status in law.

**So, arguably, the incentive for the banks to look after your money, legally speaking, has been degraded.**

Yes, and there are very precise reasons for this. The relationship between a bank and its customers is governed by contract law. The terms and conditions of that contract may be intractable, both from the point of view of length and readability. For example, Apple's *iTunes* terms and conditions extend to 20000 words. On the web, if you check a box to say that you agree to terms and conditions, the law says that you are bound by them. You should read and understand them, but that's another case where it's impractical to do so. Any organisation can then use terms and conditions to their advantage. For example, if there is a clause in your contract that says that you must never write down your PIN, and it's demonstrated that you did, the bank might refuse to make good your loss in the event of a fraud. They would be ill-advised to do so though, as they would

not want to gain a poor reputation. Also, the customer is protected against unfair contract terms by the Consumer Rights Act 2015.

A further issue has emerged recently. In 2014 the High Court heard the case of Crestsign versus Royal Bank of Scotland and NatWest. Crestsign is a business customer who entered into an interest rate swap with the bank. The idea was to protect the customer in the event of an interest rates rise. But the interest rate fell and Crestsign terminated the agreement, thereby incurring a large termination fee. The contract said only that such a fee might be 'substantial'. The consequence of this case is that the bank does not owe the customer a duty of care, in the sense that they don't have to tell the customer about anything that they didn't ask about. The bank only has to answer questions put to them truthfully and honestly. This is in contrast to organisations such as architects, doctors and solicitors, who do owe a duty of care to their customers. The Crestsign case was settled out of court in February 2016, so the law is unchanged.

**But if we circle that back to what you were saying earlier – this idea of removing passwords and making security protection based solely on software algorithms like voice recognition, of which the customer cannot protect in a traditional sense – won't this solve the problem? Wouldn't that shift liability back to the bank?**

Let's hope so. Liability needs to be placed back with the bank and away from the customer, and that's the way that the banks should protect their customers.

**Dr. Peter Mitic**, currently Head of Operational Risk Methodology at Banco Santander UK. He is responsible for model building for AMA operational risk R and statistical research, and is researching into methods for quantification of Reputation Risk.

# PROTECTING FINANCIAL DATA FROM INSIDERS

## *With insight from banking security risk expert, Patrik Heuri*

*Disclaimer: The individual views and opinions expressed in this article do not necessarily represent those of Cyber IQ or any other organization.*

When it comes to information security in the financial services, the insider threat has become something of a bogeyman. It is not simply a case of rooting out those with a lax approach to security or basic cyber hygiene; a greater awareness of the value of data means those who have access to it can be more tempted to steal or sabotage information if they become disgruntled or seek to illegally profit. Knowing whether others in your tent are doing their part to secure critical data is certainly a difficult ask, but is one that organisations are trying to solve on two fronts: better training and better technology.

*Cyber IQ* sat down with Patrik Heuri, a global head of security risk at a major bank, who confirmed that both negligence and malicious activity are being considered as equal evils.

"Recent data leaks in financial services that have been found to be intentional have created an anxiety over people risks," he says. "So when it came to delivering concrete solutions and litigation, all the issues surrounding negligence and accidental manipulation are now falling under the same treatment of processes. These recent events have clearly been driven by malicious intention, and the attention of senior management – all the budget to counter this problem – has come through that channel, for that purpose. However, in developing these improvements, we've been very happy to completely review the negligence side of human behaviour in the same breath."

> 'Non-secure data is now one of their top five risks to financial services.

Until recently, negligence and all accidental incidents were overseen by IT incident management. Now, some organisations are treating both the malicious and the negligent cases under *security* incident management, which involves increased responsiveness to

standard IT measures. This makes sense because when an employee neglects a rule and something goes badly wrong, evidence still has to be gathered and the 'scene' still has to be secured just as in a criminal circumstance. A common IT incident, on the other hand, may only require a quick fix and may not even be logged.

"We just developed a new framework for this," Heuri says of his own bank. "Covering both sides of the coin in this way is proving a quick win. By being treated within the malicious activity framework, we're seeing some good results, a better resolution timeframe, and less of an impact to day-today operations."

While efforts are being streamlined to counter the problem, the root causes behind the apparent rise in the insider threat appear to be more complex.

"I see two causes for this trend," Heuri says. "One is an increased level of frustration among employees. This is in accordance with a lower level of general treatment that many employees experience from their employers. As a matter of consequence we do see an increase of people trying to steal information.

"The other is in the way we are introducing new monitoring systems. Through greater monitoring, you get more tickets and more alerts, so an artificial statistic emerges in which more incidents are being reported."

In other words, there is some positivity to be found in the statistics, indicating that while disenfranchisement or disloyalty is perhaps more prevalent, technology and procedure is simply making it easier to notice insider problems.

## The new road

A debate has been underway in the InfoSec space thanks in large part to previous high-profile failings. Some have been arguing that the conventional approach to tackling the issue has been systems-security focused, whereas the evolution of the digital space and the extent to which data now travels beyond office-wide systems (such as on personal devices) demands that the security focus should likewise transit instead to the data itself.

> Data protection doesn't stop at the traditional company staff level; it extends further into securing home systems.

"I do believe that's exactly the model we're beginning to move towards," says Heuri. "We do have that increased risk because of the inevitable link between people and how much data they have access to, but clearly the data itself is – or should be – the main focus now for these institutions. Sometimes organisations have very complex processes or databanks, and it's just as complex to track a clear path of where the asset is when it comes to securing the data.

"If you take the broad view, financial services are now very committed to securing data and it's shown to be one of their top five risks. It's a rise in what we call 'cyber anxiety'. Organisations would like to secure both the information and the assets all as part of an information protection framework."

With that type of integrated setup, an organisation can get a better picture of all its systems, processes and IT technical controls in one place. This allows for more control of data and in an automated fashion, enabling complete alignment when building in new systems or transferring skilled people into new departments.

## Training

Today there is an unprecedented level of commitment to information security training. Data protection onsite and off is not all down to immediate operational staff. Upper management and third parties are often in need of access to sensitive information and simply locking up shop is impractical. Therefore, upskilling the entire ecosystem of data handlers is a must.

While employees are made aware of the risks through rules, policies, guidelines, education the initiation has to come from the board. Senior management has to be involved with this domain because the risk to them is now much greater, with more frequent reporting to the regulators to prove they are upholding standards and more serious financial repercussions for failing to meet them.

Heuri adds: "The clients themselves also need to be educated because often they can be the cause – or at least part of the problem – so they need to be trained in a more attentive manner, such as with fliers, classes, informal training courses, and so on. I would say they do appreciate that level of support from their financial institutions.

"It also needs to involve employees' families. Data protection doesn't stop at the traditional company staff level; it extends further into securing home systems and ensuring others around you are aware of the rules and the risks.

"So, really, you have four areas where you need different levels of education as the risk at the information security domain is amazingly universal. It's put us in a completely new playing field in terms of raising awareness."

Although the benefits of training and standards are on their way, training models are not yet mature enough in general to improve prevention and detection of data leaks. Many organisations react to problems on a case-by-case basis and so lessons also tend to be learned only on a case-by-case basis, feedback is difficult to evaluate, and results hard to quantify. Most courses, as discussed in our recent article on wider cyber risk issues, are frequently styled as checklists – 'to-dos' and 'not-to-dos', which are rarely refined, updated or embedded.

## Technology

In terms of technology, financial services – and indeed many other industries – are investing more than ever into new products that seek to weed out the insider threat before it can take effect. As an example, the upswing in employee monitoring software and analytics, designed to read patterns and flag the potential for disruptive behaviour, is no longer a niche tool. That aside, many still see a lack of innovation when it comes to solving this problem in other, less intrusive ways.

"Most banks are using existing systems that were designed to do something else and have simply been adapted for this domain," explains Heuri. "There is a big demand for new solutions but it's difficult to have when the risk surrounds human behaviour rather than machine activity. My current organisation uses a mixture of every product rather than applying a unified product that can fit all our requirements.

"In terms of Data Loss Prevention (DLP), most of the banks have tools that are in some ways an evolution of the tools that they've been using for logging and monitoring of user activity and compliance on the system, but it's still a case of adapting the old world – controlling systems rather than data – in order to try to mitigate human risk."

Hopes of progressing these tools in an integrated fashion may demand continued involvement from all parties involved in the InfoSec arena, including university researchers, law enforcement agencies, and even psychologists. However, the rate at which unified tools can be designed, tested, produced, emplaced and vetted will, for the time being, lack the speed needed to meet the most immediate or sophisticated threats, so an approach that involves plugging in smaller, verified solutions may continue to be the preferred route in the years ahead.

"It's amazingly complex to get these tools right," Heuri says. "They can't be purely IT products. They need to look at human behaviour, analyse habits, interpret data, auto-correlate trends, and so on. I believe we'll still be a bit behind when it comes to getting these tools to predict or prevent problems before many incidents occur, but they will bridge this gap gradually.

"For the past few years, we're always seeing a threat that's more advanced than the solution, so I'm not sure the gap will be closed soon, but I would love to see some dedicated companies that will really work on people and insider risk, just focusing their efforts on something that could possibly be close to the needs we have today.

"Developing something in a silo by a bank or by a law enforcement agency means we are developing thousands of the same ideas and solutions instead of putting that all together and moving faster. We have the same goals so it makes sense that we need to intensively exchange information. We're working in a regulated environment so we know exactly what we can exchange, and clients love to have a completely transparent interaction. There should be a unified approach to think about scenarios – particularly fraud – about what the next threat may be, and to be one step ahead. That's my vision – let's break down the walls."

> My current organization uses a mixture of every product rather than applying a unified product that can fit all our requirements.

**Patrik Heuri** has been responsible for Information Security Risk in private banking institutions for more than 15 years. He has developed a best in class preventive threat management of people security risks and has a holistic experience in risk that includes credit, market and operational risks.

# CONTACTS

**Editor**
Richard de Silva

**Editorial Contact**
enquiry@defenceiq.com

**Marketing Manager**
Sumit Dutta

**Advertising Manager**
John Kearns
john.kearns@iqpc.co.uk
+44 (0) 20 7368 9357

***Cyber IQ* Sponsorship Manager**
Alex Darby
alex.darby@iqpc.co.uk
+44 (0) 20 7368 9362

**Event Attendance Enquiries**
+44 (0) 20 7036 1300

IQPC, Floor 2,
129 Wilton Road,
London, SW1V 1JX

The entire contents of this publication is a copyright of *Cyber IQ*, a subsidiary of IQPC, and cannot be reproduced in any form without permission. The Editors are happy to receive original contributions to for future issues. Please note that all material sent to the Editors is forwarded at the contributor's own risk. While every care is taken with material, the publishers cannot be held responsible for any loss or damage incurred. All material rates available on request. Submitted material (especially illustrations) must be provided in digital format and must be provided with the contributor's name and contact details, including email address and telephone number. All rights to submitted material must be owned by the individual submitting. All items submitted for publication are subject to our terms and conditions, and may be amended to meet our editorial standards. For a full list of editorial guidelines, please contact the editors at the email address listed. above Cyber IQ and IQPC accept no responsibility for the continued accuracy or use of the contents of this publication. All information is subject to change.