AN INDEPENDENT SUPPLEMENT BY MEDIAPLANET

MAY 2015 CYBERSECURITYINFO.CO.UK

MEDIA PLANET

WATCH Fintech Finance interview Frank Abignale

INSIDE The threat of cybercrime on financial services **P5**

ONLINE Expert panel: The experts provide their advice

Cyber Security

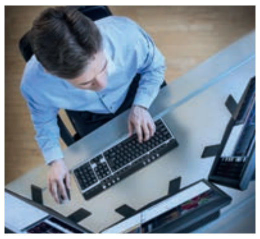
PHOTO: NEYDTSTOCK / SHUTTERSTOCK.COM

Are you prepared?

How to avoid becoming the victim of cyber crime

IN THIS ISSUE

READ MORE ON **CYBERSECURITYINFO.CO.UK**



The business case for cyber security

Despite increasing reliance on the internet to conduct business, security still does not get the level of attention it deserves.

Whether due to the misperception of cyber security as merely a function of the IT department, or the myth that a business is too small a target for a cyberattack, many organisations lack a unified and coherent cyber security strategy.

Cyber security remains a reactive action for far too many companies, despite the high chance of being attacked. For far too long, cyber security has been spoken about in negative terms, instantly scaring many senior executives into taking rash action without a comprehensive understanding of the different cyber security risks and how they affect their company.

Instead, cyber security should be seen as a business enabler. By seeing the information security of an organisation as a business problem, and not just an IT problem, senior executives can devote the same level of attention to cyber security as they do conventional business risks. Just like other business problems, ineffective cyber security can affect a company's reputation, consumer confidence and, ultimately, share price and profits.

Businesses, especially SMEs, must accept that cyber security precautions are an inherent part of doing business in today's digital world and prepare themselves accordingly.

Gordon Morrison
Director Tech for Government, techUK

"The question is not if a company will face a cyber attack, but when"

Recent research from the Cyber Streetwise campaign found that SMEs were most likely to fall for common misconceptions about cyber security. Over 20 per cent stated they believed small companies were not a target for hackers. This could not be further from the truth - SMEs are seen as a bigger target since they typically do not have the same level of protection that larger companies have in place. As SMEs become ever more reliant on web-based tools this mind-set must change.

The cyber security story emanating from SMEs is not all doom and gloom. Many of the most recent innovative cyber security solutions have come from SMEs and cyber start-ups. With the rapidly growing and evolving cyber threat, these innovative solutions are crucial to ensuring that the UK remains a leader in cyber security solutions.

However, these innovative solutions will not be utilised to their full capability if organisations are not made aware of the vast business benefits that are available to them if they ensure that they are cyber-secure. This requires cyber security to be taken seriously from the IT department to the boardroom. ■

Follow us MediaplanetUK @MediaplanetUK @MediaplanetUK Please Recycle

Managing Director: **Carl Soderblom** Content and Production Manager: **Brogan Wright** Designer: **Vratislav Pecka** Business Developer: **Alex Williams** Project Manager: **James Grant** E-mail: james.grant@mediaplanet.com
Mediaplanet contact information: Phone: **+44 (0) 203 642 0737** E-mail: **info.uk@mediaplanet.com**

Gartner Security & Risk Management Summit 2015

14 – 15 September | London, UK | gartner.com/eu/security

Manage Risk and Deliver Security in a Digital World

GARTNER PREDICTS:

> “By 2017, 30% of threat intelligence services will include vertical-market security intelligence information from the Internet of Things.”

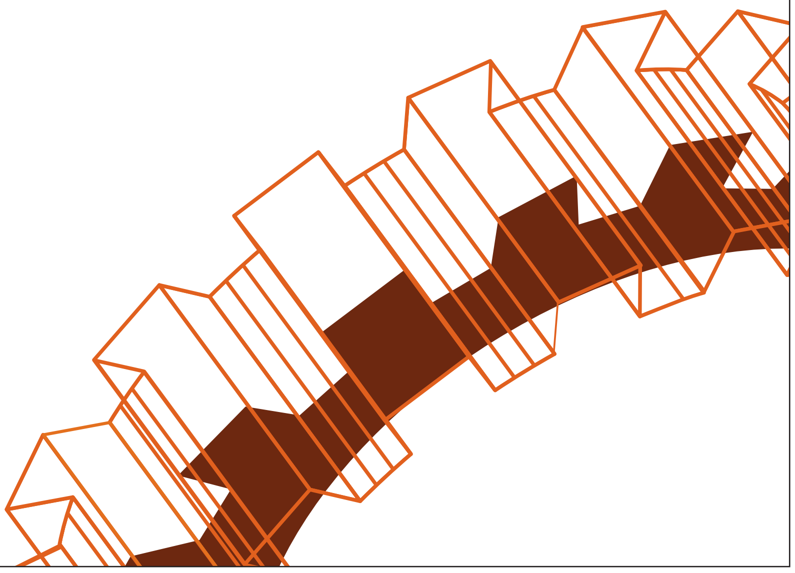
Tracks

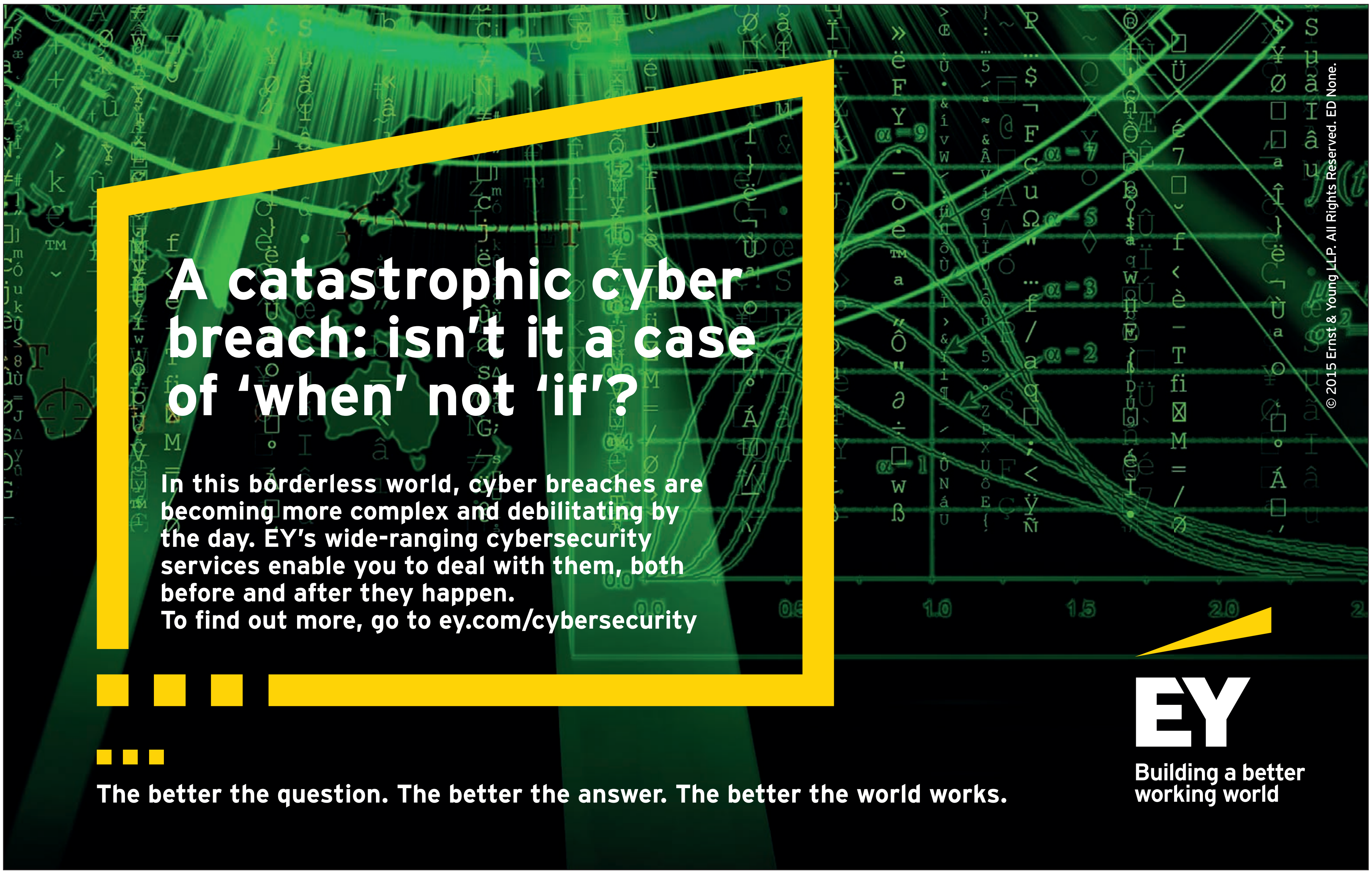
A. Chief Information Security Officer (CISO) Program

B. Risk Management and Compliance Program

C. Security Manager Program: Technology, Trends and Operations

D. Business Continuity Management Program and the Internet of Things Security Program





NEWS

Cyber security when everything is connected: We ask the experts what the future holds for enterprise cyber security

The complexity of existing software means that updates are often adopted sluggishly. What can be practically done to remedy this?

"The first step is to have a clear understanding of your software ecosystem which enables you to focus on specific updates. The adoption of enterprise rather than solution architecture roadmaps will formalise within an organisation an understanding of what software exists and what business processes it supports. Understanding this enterprise architecture and solution roadmap will ease the adoption of a risk based approach which can significantly speed up the process by reducing the need to implement unnecessary updates and the associated effort.

With this approach updates can be risk assessed by the organisation itself using industry ratings while taking into account the other defences that are in place. Updates can then be appropriately prioritised according to the risk to the organisation and implemented in suitable time.

Business strategy

In the longer term an upgrade cycle should be established which targets upgrading systems prior to their end-of-life. An enterprise architecture approach allows for appropriate budgetary planning and upgrades to be put in place ahead of time. This avoids running exposed systems or paying for expensive extended support whilst rushing a complex upgrade as was evident when organisations rushed to change from Windows XP in April 2014.

The internet of things has a wide range of applications across a series of different industries, but is the security infrastructure of major organisations sufficient to justify its widespread adoption?

"I believe that the widespread adoption of the internet of things is inevitable as connectivity becomes ubiquitous and therefore I would turn the question around - is the security infrastructure of your organisation ready for the widespread adoption of the internet of things? There are many opportunities for the public as well as private sector, new innovations are being introduced daily but along with these, threats are being created which will challenge your organisation. Information sharing and ease of accessibility particularly to operational technology via the the internet of things makes businesses vulnerable to targeted cyber-attacks, however the potential benefits are high.

Julie Evans
Executive director cyber security & resilience, EY

If organisations fully understand their existing eco-system and deploy appropriate controls, the risks can be minimised. The potential risks and impact of system compromise and data leaks must be identified and assessed for each internet of things opportunity for the organisation and its partners. The "defence-in-depth" approach should be implemented as for any end point attached to your network. Exploit tolerant networks, systems and rapid detection and response are central to the successful and secure adoption of the internet of things, but rely on investment being made to examine the security as well as the enabling capabilities of internet of things devices.

"Recently there appears to be a growing appetite for using a single consolidated provider that can offer all the cyber security services an organisation may require"

Read more at **cybersecurityinfo.co.uk**

Do you see enterprise approaches to security becoming more individual and diverse, or consolidated amongst a series of global providers?

"Historically organisations have been using multiple providers leading to unique security approaches and given the unique nature of the infrastructure of large organisations. Recently, there appears to be a growing appetite for using a single consolidated provider that can offer all the cyber security services an organisation may require. However, whether an organisation uses multiple providers or a consolidated provider, it is vital that the services procured match the risk profile of the individual organisation. The organisation must also risk assess the providers they use as the provider represents another attack vector for an attacker and could negate the value they add. The differing attitudes to supplier consolidation can often match corporate risk appetites, as risk-averse organisations will seek to spread their risk across multiple suppliers to lessen the impact of a critical failure whilst risk tolerant organisations may consider the cost savings often achieved. ■

How is cybercrime and fraud a threat to banking and financial services?

By Ali Paterson, Fintech Finance

As part of a recently released video for Fintech Finance, I had the pleasure of speaking with Frank Abagnale JR, famed for Leonardo DiCaprio's portrayal of him in 'Catch me if you Can'.

Frank Abagnale JR (on left)
Subject of the movie 'Catch me if you can'
PHOTO: FINTECH FINANCE

However one of the most interesting things about Frank is not his past endeavors but his current work, contributing to the future of preventing cybercrime and fraud. "The two biggest things right now are, firstly a lot of account takeover where a CFO sends an email to wire 'X' amount of money to a certain client or customer and someone does that exact email over and over again. Secondly, and this is very scary, the amount of breaches; we're having almost one everyday – not just banks, any company that keeps data so doctors, law firms, anyone that has data with information that people want. They're deadly in the fact that even if you don't lose any money, the reputation and the fact information has been stolen about your clients is devastating to ones stock. What's scary is a lot of the time they don't tell their customers to change their passwords even though a breach has happened."

Frank's warnings are reinforced when later I spoke with Amit Shah, head of multi-channel analytics at NICE systems. "It's all about education for the public" states Amit, "banks need to make customer aware of fraud threats. It's about awareness, not just making sure relevant solutions are in place, but to actually protect customers and make them aware of what's happening."

In an era of constant financial regulation, there is very little when it comes to security regulation; "There are no compliance stipulations at an industry level" says James Cronk from Cisco, "unless a bank is recognised as a critical infrastructure, there is nothing that is actually regulated for them, so it's best practice, guidance and how they view things themselves."

Informing the industry on best practices is one of Frank's passions. He recently delivered a seminar to a large UK bank emphasising the importance of educating its staff on security. He purposely planted a number of USB drives marked 'Confidential' in the car park and nearby vicinity, to find an hour later, almost all of the USB drives had been connected to the banks network. The implications being that any form of virus,' Trojans or smartwear could have been on those USB's posing any number of catastrophic threats to the bank's systems by it's own employees.

So what can be done about it? Frank focuses on data analysis; working with the FBI, developing systems that not only monitor the pin number you enter at an ATM, but the speed and pressure that it is entered; which combined with your phone GPS location and your past ATM history, have the potential to detect when something is awry.

NICE focus on the progression of technology. It becomes increasingly apparent that passwords alone have become somewhat archaic and insufficient in protecting users. They propose a future where voice and palm biometrics become the norm, "taking away the burden of being asked millions of questions ' and we, as the general public would be safer for it. These measures are organic; as advanced as they are, they will never be 'the answer', as cybercrime continues to evolve so must the security measures remain dynamic in order to stay one step ahead.

In conclusion to these interviews it seems that the most progressive thing a bank can do right now is admit that there is a problem. Frank acknowledges that "these things are becoming more and more common and they don't get made public because banks don't want to admit they lost the money." Whilst technology continues to advance in a cybercrime vs. cyber security battle, education of banks and their customers is key. ■

Gareth Niblett
Chairs the Information security
specialist group of BCS, The Chartered Institute for IT;
provides security, privacy and compliance advice through
Blackarts Limited; and tweets as @garethniblett

Security Analytics

The growth in big data solutions is allowing the emergence of big analytics. This involves taking the data collected and exploiting it to get useful answers. One key area benefiting from this is security analytics. Historically, security tools were limited to performing transactional queries, looking for simple pattern matches, to identify possible attacks. Now we can run more complex, wider-ranging queries to identify trends and patterns we might not otherwise have detected.

We can now pour in high volumes of various data formats at velocity, without the stumbling blocks of a data warehouse project, around export, transform and load. Data scientists can now dive into a data lake, where there is flexibility in the database and data, to pull out previously impossible (or a least challenging) results. They can form a hypothesis and test it against a large dataset, rather than trying to target and gather specific data to answer a known problem.

New rules can be developed, to allow for the automation of security analytics, helping with areas of security operations, including protective monitoring, privileged user monitoring, web fraud detection / transaction monitoring, threat intelligence and the wider situational awareness piece. Beyond relying on smart data manipulators, machine learning will emerge to help crunch through ever-growing data, to help inform human operators, or even automate responses.

Wherever the coming years take us, the world of security analytics is going to progress at pace and bring in a new generation of data analysts, tools and data. ■

PHOTO: THINKSTOCK

Hands on learning. Awareness training is becoming essential for organisations

Companies are falling short on awareness training

Clicking on a web link in an email is a common and often harmless task that we all do every day both at home and work.

Yet, as we have been told, and have seen, it can actually be very dangerous and can lead to massive problems for individuals and companies. Cybersecurity professionals call these sorts of attacks, for that is what they are, phishing attacks. These attacks refer to a multitude of clever scams that aim to lure people into launching malware or offering information that an attacker can use to compromise systems, steal data, or mimic identities. They can range from fraudulent phone calls from people pretending to be from your bank, utility, or helpful service desk, to emails that invite you to hold money for people trapped in warzones or confirm your bank details. And they can be very clever. People who have long understood the concept of a phishing attack are at risk of being duped as these attacks become more targeted, even personalised within email invitations, in texts and on social media sites.

These cyber security scams have become headline news and many companies recognise the need to invest in programmes to help their employees be more aware of the risks. It comes as a worrying surprise therefore when phishing scams top our list of tactics that security professionals are facing today.

Adrian Davis, CISSP
Managing Director EMEA, (ISC)2

Our 2015 Global Information Security Workforce Study conducted by industry analysts Frost & Sullivan surveyed nearly 14,000 information security professionals around the world to reveal, predictably, that the threat techniques employed by attackers and hackers today are diverse. Phishing attacks featured prominently as a top concern identified by 54 per cent of respondents, way ahead of other concerns such as network malware (36 per cent). According to the study report "the realism and targeted approach of today's phishing campaigns appear to rival the information security professional's efforts to elevate employees' ability to recognise, report, and leave untouched suspected phishing messages." This is worrying given how just one mistake can lead to a virulent propagation of malware across the organisation's network and systems.

A rising threat

Data Breach Research from Verizon confirms a rising trend, with phishing being in the top 20 varieties of threat actions in each of the past five years, rising to tenth place in 2013 and then third last year. The rise of such threat actions is also driven by the sophistication of attacks, with the information gained in phishing scams often used to compromise systems utilising other techniques, in what are known as Advanced Persistent Threats (APTs).

> "These cyber security scams have become headline news and many companies recognise the need to invest in programmes to help their employees be more aware of the risks"

What are companies doing to cope with this risk? Investments are being made in tools and technology. However, creeping levels of complacency around awareness training may well be a contributing factor in making phishing attacks effective. Our survey, which has been conducted for over ten years, shows a declining trend in respondents indicating demand for end-user education and training over the past three surveys (2011 - 39 per cent, 2013 – 38 per cent, and 2015 – 32 per cent). Further, there is notable downward movement in the levels of concern associated with mobile devices and internal employees. It's not that the concern isn't there, but other concerns are rising up the priority list.

With regard to awareness, I worry that companies and organisations may believe that they are doing enough, or worse, believe they have already taken care of the need with online training resources or the programme delivered last year. The hackers' success should puncture this complacency. The reality is that delivering awareness training isn't enough. Appropriate security instincts, which starts with a recognition of accountability, must be embedded across the organisation. Common awareness techniques only go so far. There is considerable work ahead for organisations who must assure an understanding of how this can be accomplished in their organisation; assuring their efforts are highly contextual and relevant to their risks. The first step will be recognising the priority. ■

Learn more at
cybersecurityinfo.co.uk

Tackling the cyber security skills gap

Lieutenant General
Sir Edmund Burton KBE
Chairman of the Information Assurance Advisory Council (IAAC)

"The Government has a vision for a vibrant, resilient and secure cyberspace, contributing to economic prosperity, national security and a strong society. The vision can only become a reality if we have a strong cyber security skills base in the UK, both within Government and in the private sector." [Minister for Universities and Science - March 2014]

This vision calls for urgent action by executive boards across public and private enterprises, in partnership with schools, colleges and universities. The initiative presents national and international business opportunities for enterprises large and small. Previous national initiatives have failed because of a failure of executive boards to engage and to provide the necessary leadership and resources.

The national need can be met by focussing national efforts around the Government Cyber Security Skills initiative. Such a programme already provides a clear statement of the objective that has instigated a range of concurrent activities. These have included the recent changes in primary and secondary schools' curricula and the establishment of cyber security centres of excellence in research and education.

While the UK addresses the medium and long term need for skills and education, there are major opportunities for the providers of managed security services to meet the current, urgent and important needs of enterprises. This will achieve the cost effective management of persistent threats to businesses and should result in the development of a discerning and intelligent customer community.The success of this historic opportunity will depend on the effectiveness of leadership, by example, throughout public, private and third sector enterprises.

Learn more on
cybersecurityinfo.co.uk

COMMERCIAL FEATURE

Mind the gap - the cyber security conundrum

Imagine that you've just invested in a brilliant new security tool – there it sits, full of promise – but unless your staff know what it should be protecting and how to use it, it's little more than a giant paper-weight. That's how many companies are traditionally tackling the cyber security threat – by using technology to fix a problem.

When combating the ever growing cyber threat, it's commonly accepted there is a requirement for people, process and technology, but all too frequently companies put most emphasis on the latter. Whilst this is proving a successful way to increase budgets as leadership can easily conceptualise the need for a solution they can touch and feel, the skills gap that subsequently occurs tends to be overlooked.

In KPMG Cyber Academy's survey[1] of 300 senior IT and HR professionals in the UK 74 per cent admitted their new security challenges require skills they didn't currently have, whilst 64 per cent believed the cyber skills needed are significantly different to those used in traditional approaches. These figures do beg the question as to why there is now a skills gap when the field of information security has been around for many years. Has the landscape changed that much or is our dependency on technology forcing a reliance on specifically skilled professionals?

Whilst the debate to find the answer will, no doubt, continue for some time, the problem remains unresolved. So how can we begin to fill the inevitable skills gap? Three common areas of consideration are hiring, upskilling and outsourcing, but, as is so often the case, the answer depends on the appetite of the company in question.

Matt White
Head, KPMG access manager,
matt.white@kpmg.co.uk
Twitter: @cybermattwhite

Some have turned to hiring ex-hackers to bridge the gap and whilst a seemingly simple solution, this has its own inherent risks with the simile of 'poacher turned gamekeeper' springing to mind. Further complications arise with 57 per cent of those surveyed saying it had become more difficult to retain specialised IT staff in recent times. So is there a better choice?

To the cynical, upskilling is often seen as simply providing more training for IT staff so that, amongst other things, they can increase the number of letters after their name. However, if taken as part of a structured firm wide cyber awareness initiative involving everyone from the C-suite to graduates, the results can be profound.

Last but not least is outsourcing, an option that for years has been immersed in a culture of cost cutting and efficiency benefits. However, when faced with a lack of technical security skillset the application of managed services can provide significant returns. For example, an identity and access management programme is a potentially labour intensive and specialist field, but by removing the need for continued development or recruitment of information security personnel, a trusted outsourced provider can deliver a level of comfort and assurance.

Further benefit can be taken from outsourcing as it potentially reduces the likelihood of someone exploiting their access rights, something 60 per cent of UK CIOs surveyed in KPMG's 'Trust Paradox'[2] believe will come from within their organisation.

[1] KPMG in the UK's Cyber Academy's 'Cyber Skills Gap Survey' October 2014 http://www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublications/NewsReleases/Pages/Hire-a-hacker-to-solve-cyber-skills-crisis-say-UK-companies.aspx

[2] 'The Trust Paradox: Access Management in an insecure age' February 2015, CIO UK in association with KPMG in the UK and RSA. http://www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublications/Documents/PDF/topics/the-trust-paradox.pdf

COMMERCIAL FEATURE

The Human Factor - Lessons learned from staff training and policy management projects

According to the findings in PWC's "Global State of Information Security Survey 2015," the annual average financial loss attributed to cyber security incidents was estimated at $2.5 million, a jump of 34 per cent over 2013. No one doubts that the digital security posture of an organisation is now a board level issue, and that's a big change from five years ago. However, executive anxieties need to be matched with a long-term structured strategy that everyone in the company ecosystem is willing to invest in so that the highest standards of information security are maintained. Inevitably, this will require a change in company culture as most staff members view this issue as belonging to the IT department. They often forget that the consumption of IT Services is often the point of maximum vulnerability for the company. It is here that the user can compromise the security of the company by becoming a victim to phishing tactics or acting in an inappropriate or negligent manner, regrettable situations that expose the organisation to cyber risk.

So what are the lessons we can learn from implementing an appropriate strategy to changing human behavior in this area?

Well the first is to recognise that changing culture in information security practices is no different than any other change management process within a company. It is as difficult as any other change management process requiring significant effort and resources to make an impact.

Another lesson is that quality matters. Too often staff security training is a ticking the box exercise, with very little energy being expended on planning or on content. The latter is one of the most important considerations in determining the success of a culture change initiative. Take eLearning content for example. The industry is awash with boring, bland, and often dumbed down IT Security training courses. It is no wonder that there are cases of low staff participation that necessitate significant management intervention. ELearning courses should reflect the digital threat that we all need to combat.

Robert O'Brien
CEO, MetaCompliance
www.metacompliance.com

Another key lesson is ensuring the correct targeting of high-risk groups. Rather than "blanket bombing" all staff with general cyber security communications and policies, organisations should identify high-risk staff groupings and provide tailored messaging and surveying. Examples of these staff groups would be privileged users, such as administrators and information asset owners. Clearly, the communications sent to these high level positions would be more detailed than what would go to the overall user population. In many cases companies are struggling to get messaging out to everyone. So a shift in priorities is required.

Be prepared for the long haul. The changing of IT Security culture is a multi-year project. It's not possible to deliver all the policies and education that are required in a short period, as the user base will become fatigued. The best approach is to build up your communications over time. Obtaining outside expertise to assist in the crafting of a fit-for-purpose communications initiative is one way of jump starting a moribund security staff training programme.

So let's accept that email, Share Point and corporate intranets are not suitable for obtaining active staff participation in proper staff awareness activities. They require significant management intervention to ensure that staff members undertake their commitments to mandatory policies and eLearning. A more appropriate approach would be to adopt best in breed automation that actively engages the user and provides the necessary reporting needed for certification and regulatory review. ■

40,000 BUYERS AND BUSINESS PARTNERS

@IFSEC #IFSEC2015

IFSEC International

SECURING PEOPLE, PROPERTY & ASSETS

Access to leading global technology, solutions and knowledge to enable security excellence

PART OF PROTECTION & MANAGEMENT 2015
UNITING PROFESSIONALS ACROSS SECURITY, FIRE, SAFETY, FACILITIES & SERVICE MANAGEMENT

16-18 June 2015, ExCeL London

Photo courtesy of: Crossrail

- Hear from industry leaders on how we are securing our cities at the Safe Cities Theatre
- Meet international thought leaders at the Euralarm conference
- Pre-book meetings with your preferred suppliers through the Global Meetings Programme
- Get all your security solutions, education and training in one place

REGISTER FOR YOUR 2015 BADGE TODAY at www.ifsec.co.uk/cityAM

The global stage for security innovation and expertise at ExCeL London, 16-18 June 2015

Supported by

bsia british security industry association

NSI Security.Improved

SSAIB

HYPER/CAT

Organised by

UBM