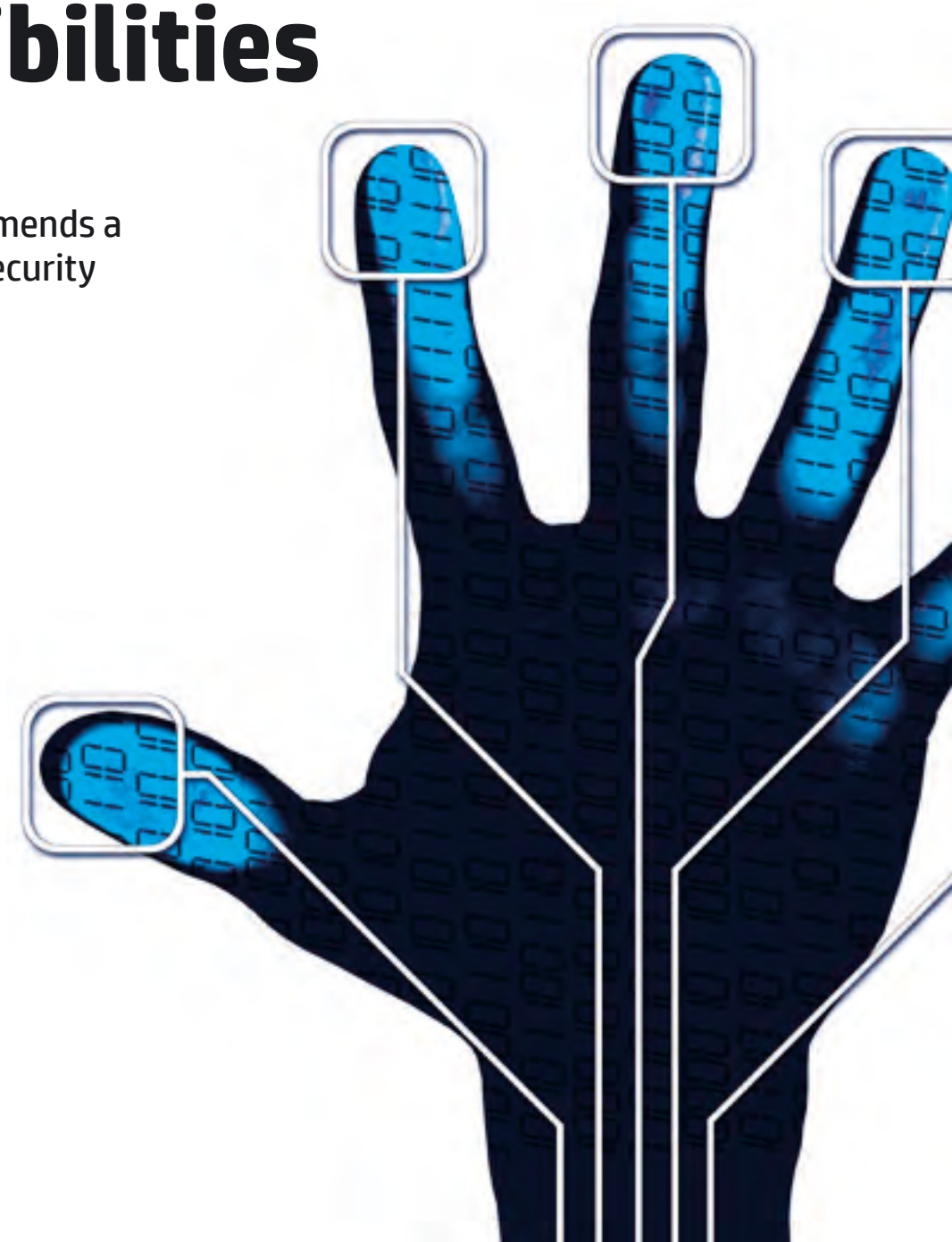
Inform

From HP Enterprise Security Global Issue 8 2012

Step up to your digital security responsibilities

Raja Azrina of Jaring Communications recommends a top down approach to security



Consumerization

Make your security move with your data.

Getting to grips with Social Media

How to securely manage social media in the enterprise.

The SIEM Advantage

Security Information and Event Management (SIEM) as an essential tool for security professionals.

Inform.

Learn more, act quicker and make it matter

Keep up to date with the latest and greatest from the Information Security world by subscribing to HP's Inform magazine.

Inform Magazine is a quarterly publication designed to give you a wealth of insight on current topics from key industry figures. It has contributors from all over the globe, covering many different industries and sectors.

Regular features in each issue include:

- Key thought leadership interviews with senior IT Security professionals
- Current news and hot topics
- Practical how to guides
- Latest technology updates

And much more...

To view past issues please visit **issuu.com/hpenterprisesecurity**

Subscriptions are complimentary for CIO, CISOs and IT Security professionals. To subscribe please send your details to **hpinform@hp.com** detailing your name, title, company, email address and country location. Please include your postal address if you would like to be sent a hard copy of the publication.

Please let us reiterate that HP is committed to respecting your wishes for privacy to the very best of our ability. Privacy is an important issue to Hewlett-Packard that we take very seriously we believe strongly in consumers' rights to manage and protect their personal information. Your information will not be shared outside HP unless you give your consent. You can choose whether HP may communicate directly with you. For more information please see the Privacy Statement.

In this edition

Welcome

Writing this column for Inform I was struck by the gathering pace and sophistication of cyber attacks occurring across the world. The news reports on the Flame virus that emerged in May this year were alarming indeed.

According to experts, the degree of sophistication of the programming that went into this latest piece of malware is like nothing we have seen before. It's at an unprecedented level. If there was any doubt, there can be none now that we are entering a new and very dangerous era where enterprises and even entire nation states are at risk from cyber weapons designed to destroy infrastructures. Even if such an attack is highly targeted initially, the impact of the malware once in the wild is likely to be far wider and hugely difficult to control.

Where does that leave HP's customers now facing these challenges? As this issue of Inform clearly demonstrates it isn't just the threat of cyber attack that C-level security leaders have to meet head on. The unstoppable rise of consumerization and smart device penetration into the enterprise, politically-motivated hacking and cross border data protection legislation that cannot be ignored remain firmly on the agenda. And of course all of these challenges must be met against ongoing budgetary constraints as the global economy continues to stall. A tough call, and at HP we understand that.

I travel the globe meeting our customers, technology partners as well as HP's own experts to better frame our response to these huge challenges. And our response is not just one of existing technology solutions but increasingly research and development programmes dedicated to building next generation, intelligent "hyper defences". This is not just a commercial decision. Like other vendors we believe that if we are to stay ahead of the threat and the attackers we need to co-operate and share intelligence.

We have at our disposal technology white papers and thought leadership pieces written by HP security and information experts based at centres of excellence around the world. As we seek to play our part these are available to all - indeed Inform itself forms a very important part of this education piece. I don't think it's too much of an exaggeration to say that the cyber threat poses a real threat to our way of life. It's that serious.

The business world needs robust defence technology from resource rich partners like never before. At HP we are continuing to work hard to build the resources and technologies not just to deal with today's threats but those of tomorrow, which are likely to be severe and test us like never before.

I truly believe that if we are to keep on top of our adversaries we need technologists, researchers, analysts and other experts to help build new ways of working. I believe that in these difficult times you need partners that have the advantage of worldwide resources. Partners like HP.

Dan Turner
VP Enterprise Security Services

Inform
Issue 8 2012

Published by HP Enterprise Security
Web: www.hp.com/enterprise/security

For enquiries about Inform, please contact sarah-ashley.stephens@hp.com

Produced by: www.crisp-design.co.uk
Edited by: PF&A

If you would like to subscribe to Inform Magazine please contact us at hpinform@hp.com

FSC

When you have finished with this magazine please recycle it.

News

New campaign to raise security awareness among smaller businesses

The Cyber Security Challenge UK and Get Safe Online have launched a joint competition that will aim to teach small businesses about cyber security.

The campaign called 'Can you talk security?' is challenging the public to come up with ways to communicate technical security issues to small and medium sized organisations in a simple and non-technical way. The winning entry will then be posted on the Get Safe Online website to be used as a resource for small businesses and offices.

“Creative communicators might not seem an obvious requirement for a cyber team, but the need to communicate technical security issues in a way that can be understood by members of the public, employees and decision-makers in boardrooms is extremely important.” said a spokesperson for Get Safe Online.

Cyber Security Challenge UK

The campaign runs in the UK until June 22 2012.

http://bit.ly/K9aQOU

Russian cyber crime market worth $2.3 billion, global total at $12.5 billion

According to a report by security firm Group-IB, a Russian cybercrime investigation and computer forensics company the value of the global cybercrime market now stands at $12.5 billion, while the Russian national market alone stands at $2.3 billion.

According to the group, traditional crime syndicates are now beginning to organize the previously disorganized Russian cybercrime market. In addition, these crime syndicates are beginning to work more closely together, sharing compromised data and botnets.

At the same time, In 2011, the largest type of Russian cybercrime was online fraud at $942 million; followed by spam at $830 million; cybercrime to cybercrime (or C2C including services for anonymization and sale of traffic, exploits, malware, and loaders) at $230 million while DDoS accounts for $130 million.

“The cybercrime market originating from Russia costs the global economy billions of dollars every year,” said Ilya Sachkov, Group-IB’s CEO. “Although the Russian government has taken some very positive steps, we think it needs to go further by changing existing law enforcement practices, establishing proper international cooperation and ultimately improving the number of solved computer crimes.” he said.

UK health service hit by major fine for data leak, ICO shows teeth

ico.

The UK's Information Commissioner's Office (ICO) fined the National Health Service after a mental health patient's file was leaked via email.

According to reports the ICO handed down a £70,000 fine to the Aneurin Bevan Health Board in Wales for sending the sensitive information to the wrong person.

The error occurred when a consultant emailed a letter to a secretary for formatting, but did not include enough information for the secretary to identify the correct patient. The doctor also misspelt the name of the patient at one point, which led to the report being sent to a former patient with a very similar name in March 2011.

"The health service holds some of the most sensitive information available. The damage and distress caused by the loss of a patient’s medical record is obvious, therefore it is vital that organisations across this sector make sure their data protection practices are adequate," an ICO representative said in a statement.

"We are pleased that the Aneuvin Bevan Health Board has now committed to taking action to address the problems highlighted by our investigation; however organisations across the health service must stand up and take notice of this decision if they want to avoid future enforcement action from the ICO.”

The ICO was given significantly enhanced powers to fine companies for breaches of the Data Protection Act in 2011.

Largest UK data breach fine handed to health service trust

A data breach at a UK hospital trust resulted in the largest fine yet handed down by the UK data regulatory body, the Information Commissioner's Office (ICO). The Brighton and Sussex University Hospitals Trust was fined a record $210,000 for filing to secure patient data held on hard drives.

The ICO said that hard drives were sold on an internet auction site in October and November 2010 and that it had discovered "highly sensitive personal data" belonging to tens of thousands of patients and staff.

ICO deputy commissioner and director of data protection David Smith said: "The amount of the monetary penalty issued in this case reflects the gravity and scale of the data breach. It sets an example for all organisations – both public and private – of the importance of keeping personal information secure."

The fine handed down was seen as an indication that the ICO fully intends to enforce Data Protection Act more rigorously with substantial fines. The Trust said that it would appeal the decision.

Controversial CISPA act gets through US House of Representatives

The controversial Cyber Intelligence and Sharing Act (CISPA) cleared its first passge through the US Parliament in April. The bill is designed to make it easier for companies to share information collected on the internet with the US federal government in order to help prevent electronic attacks from cybercriminals, foreign governments and terrorists.

However the bill has come up against strong opposition form civil liberties groups concerend about personal freedom and intrusion into private data. According to critics, ISPs could easily turn over private communications such as emails and browsing history.

We will not stand idly by as the basic freedoms to read and speak online without the shadow of government surveillance are endangered by such over-broad legislative proposals," said Rainy Reitman, who heads the Electronic Frontier Foundation's activism.

According to a report in The Guardian, the Center for Democracy and Technology said it was "disappointed that Cispa passed the House in such flawed form and under such a flawed process."

"We worked very hard in cooperation with the intelligence committee to develop amendments to narrow some of the bill's definitions and to limit its scope. We are very pleased that those amendments were adopted, leaving the bill better for privacy and civil liberties than it was going into the process," it said.

Electronic Arts CISO warns that advanced persistent threats are here to stay

At the Infosecurity show held in London this Spring, Spencer Mott, CISO at US gaming firm Electronic Arts warned that enterprises will continue to be breached by APT attacks for the foreseeable future.

According to a report in SC Magazine he told delegates at the conference that businesses need to accept that their networks are vulnerable to advanced evasion techniques (AETs) and advanced persistent threats (APTs). He advised they move towards protecting specific assets to protect the brand.

"Eventually this threat is going to impact any significant business, although the big global brands are going to be the most-impacted organisations. This should encourage CEOs to get more realistic. This isn't just a role for security teams, it is about business processes" he said.

On a more positive note he said that it was still possible to have have defendable assets and that CISOs needed to concentrate on protecting those.

"Be in a position as and when an attack occurs, from a brand perspective at least, to show consumers and regulators you did everything you could to defend against it." he said.

Insights

HP research identifies new era of security risk and vulnerability shifts

In its 2011 Top Cyber Security Risks report, HP Enterprise Security provides a broad view of the vulnerability threat landscape, as well as in-depth research and analysis on security attacks and trends.

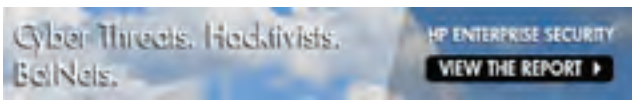
Historically, the number of vulnerabilities disclosed in a year indicated the current state of the security industry and helped organizations prioritize their defenses. However, the report demonstrates that vulnerability volume is no longer a valid indicator of the security risk landscape. While newly reported vulnerabilities in commercial applications continue to decline, a large number of vulnerabilities are unaccounted for, and are therefore undisclosed to the broader security industry.

"To protect organizations against a wide range of attacks, HP has established a global network of security researchers who look for vulnerabilities that were not publicly disclosed," said Michael Callahan, Vice President, Worldwide Product and Solution Marketing, Enterprise Security Products, HP. "The intelligence gained from this research group is built into HP enterprise security solutions in an effort to proactively reduce risk."

Simon Leech, Pre-sales Director EMEA at HP Enterprise Security, said attackers are moving to in-house-developed applications as the attack vectors are moving from opportunistic attacks to more targeted ones.

"Vendors will not have signatures to patch vulnerabilities on in-house applications. Our research found that 54 per cent of in-house applications had reflected cross-site scripting (XSS) flaws; 40 per cent had persistent XSS failings; and 86 per cent injection flaws. Protecting and fixing these applications is becoming very relevant to protecting the infrastructure," he said.

Download the full report: http://bit.ly/I90doo



HP publishes expert guide for CIOs on managing mobile devices

The world is only becoming more mobile, not less. It's a one way street and so HP Enterprise Security has produced an in-depth report into managing data loss on mobile devices. The report, 'Managing Data Loss in the Modern Enterprise', has a number of key findings that CISOs and CIOs are likely to find invaluable when formulating a secure mobilty strategy for their own organizations. For example, it reveals that demonstration of regulatory compliance is likely to be far harder with the proliferation of consumer sourced smart devices in the workplace.

It finds that employees increasingly want to use their own devices – and enterprises want to attract the top talent that reflects their consumer base. Employers want Generation Y employees who represent their consumers. Decisions around mobility are often dominated by consumer trends, especially among senior executives themselves; they are often the first to insist on being allowed to use their iPads or iPhones, even when it causes the CISO's team headaches due to the additional risks and complications to the infrastructure. Looking forward, CIOs should consider the question: 'What types of devices will be on my network in three to five years?'

The report analyses how increased mobility will impact on six key industry sectors: technology companies, financial services, retail, manufacturing, healthcare and public sector. Each will need to treat the onset of mobility in different ways. One of the key findings is that for the first time in history, technology choices within the enterprise are being influenced by fashion and individual choice – security leaders must adapt to this change. The report says: "Many business stakeholders are not sufficiently informed of the implications of technology and behavioural changes. A 'user-centric view of the world' is required moving forward.

The report concludes with a fundamental 5 step approach to mobility for the CIO that can be undertaken straightaway. Written by leading CIOs, CISOs at major corporations and HP subject experts the report is available for download now.

Download the full report: http://bit.ly/JzUSwq

What do the EU cookie laws mean for your business?

On Monday 28 May, the long-awaited EU Regulations on the use of cookies was introduced in the UK. But what does this mean in practical terms for your business? Andrzej Kawalec – CTO, HP Enterprise Services tells you what you need to know.

What are the new laws?

In a nutshell, they are quite simple. Or at least they were until 48 hours before the deadline for tabling amendments.

As the proposed law stood, any websites operating in EU member states, including foreign owned (but with an EU domain), must now get express user permission to download cookies onto the browser device be it PC, tablet or smart phone. This is part of the EU's Directive on Privacy and Electronic Communications designed to enhance personal privacy of EU citizens online. However, before it came into force in the UK, the Information Commissioner's Office (ICO) issued an updated version of its advice for how to use cookies, which stated that, for UK companies, implied consent was sufficient.

"The intention behind this Regulation is to reflect concerns about the use of covert surveillance mechanisms online"

What does this mean in practice?

The last minute change may, at first glance, seem like a wholesale lifting of the obligation but it is not that straightforward.

ICO guidance indicates that UK businesses should not assume consent has been given merely because a user has visited their website. Consent should be "specific and informed". If the website does nothing to alert the user to the fact that cookies had been set, it is unlikely that the user will understand they are entering any sort of agreement and therefore, they will not be deemed to have given valid "informed" consent within the meaning of the regulations. What "informing" the consumer will consist of, depends on factors such as the sensitivity of the information being tracked, the nature of the intended audience for the site and the way users expect to receive information from it. If, for example, a site stores a user's sensitive medical data, the steps it will be expected to take to secure informed consent will be more onerous. ▶

In the UK at least, fines of up to £500,000 could be imposed by the ICO against transgressors, whatever the source of the web site.

This change could put the UK out of step with the rest of the EU and lead to conflicts in the European courts but for now, this is how the law stands.

How often does this need to happen?

As far as individual users are concerned they need only give permission once unless the type or number of cookies changes.

Why have they been brought in?

According to the ICO:

"The intention behind this Regulation is to reflect concerns about the use of covert surveillance mechanisms online"

Translated, what that actually means is protecting the public online from illegal spy ware and misuse of cookies, intentional or otherwise. The legitimate use of cookies to, for example, speed online transactions and promote products based on browsing history is not being outlawed. Simply, owners must get permission from users to download cookies, though this need now only be implied permission.

Does anyone care?

Probably more than you think. The new directives are designed to protect the public from having personal data mined and stored without permission. The public, certainly in the UK, is very aware of data privacy issues after the News of the World hacking scandals of and major data breaches of 2011. The public is still largely unaware of the extent of cookie use on the web. A chance to reduce mistrust and isolate criminal use of spyware should be welcomed.

What are the penalties for non-compliance?

In the UK at least fines of up to £500,000 could be imposed by the ICO against transgressors whatever the source of the web site. Across the EU, however it is harder to find similar commitments to fines, which is one of the anomalies of EU directives - the lack of uniformity in dealing with non-compliance.

Cookies: the view from the CIO's office

The challenges in meeting the Directive is identifying and modifying an existing web presence so that it complies with the new rules but doesn't drive customers away and impact on the business benefit of web sites. Some CISOs think that the new directive could be bypassed by the less scrupulous. People's browsers, their operating system, plug-ins and PC set ups provide a unique footprint which meant that businesses could identify and track user behaviour without ever putting a cookie on their devices.

There is also the difficulty in dealing with customers asking for privacy online but who also have credit cards, loyalty cards where they happily give information away in return for vouchers and financial rewards. People are looking for privacy yet they're willing to give it away if it suits. ■

Links

http://www.allaboutcookies.org/

ico.

ICO guidelines:
http://bit.ly/ICOguidelines

Action points on cookie compliance

+ Identify an inventory of all the websites you have, not just those you host and manage but those managed by third parties on your behalf. If they carry your brand you need to ensure compliance.

+ Work closely with your marketing teams and audit EVERY web technique and database they use and then set up a management tool to ensure ongoing compliance.

+ Think about how to adjust your sites. For example, give users very clear information about how you use cookies and their benefits to the customer. **Cookies on as default is not an option.** ■

Need to see everywhere at once? You can.

You can't stop threats if you can't see them. Gain context-aware visibility into security risks with HP Enterprise Security's proven solutions. See how to protect your IT environment from sophisticated threats with the integrated correlation, application protection, and network defenses delivered by the HP Security Intelligence and Risk Management platform.

See everywhere at once. Arm yourself with advanced protection against advanced threats.

For more information go to
hpenterprisesecurity.com

See. Understand. Act.

Planning ahead with Check Point

The President of the Israel based security firm, Amnon Bar-Lev outlines the company's ambitions.

Amnon Bar-Lev is President of Check Point, the Israel based company widely credited with inventing the firewall. Inform caught up with him to see how the company's technology is adapting to the demands of the business focused CISO.

According to his official Check Point biography, Amnon Bar Lev joined the Tel Aviv-based company in 2005 bringing with him 15 years of high-tech sales, marketing and management experience to the organization.

He is now responsible for worldwide sales, global partner programs, business development and technical services for the company. When you're in charge of a $1.247 billion company, it is quite a responsibility – but one that he's bearing well. That revenue figure represents a 14% increase year on year. Much of this growth must come from the fact that Check Point is much more than the commonly-held perception of a "firewall company" these days, as Bar-Lev explains.

"I think we have probably the largest amount of IPS deployed in the world. And we see huge growth in this space. It's not only about perception; it's about reality, it's what people are buying from us.

And we're seeing people buying more and more things from us. That's a good start. The challenging one is that we want to shift more and more," he says.

So what is the company developing to achieve growth and meet the demands of security in the modern enterprise?

"We have an architecture called Software Blade Architecture. Now, if you want to have more security protection you don't need to download more apps, you just activate it via the management console – so it's scalable.

For example, you can control which applications are running on the networks with an Application Control Blade. Or if you want to run an IPS, you can activate that and control unauthorised access on the network. Blades are starting at $1,500 per year, so they are very affordable, and you can pick and choose on where you want to run what," he says.

Bar-Lev adds that the market has taken to this approach as the increasing sales, either as bundles to clients or stand-alone, continues to "grow very nicely".

Check Point recently unveiled a new extension to its blade offering with Anti-Bot technology. So what brought this about and what is Check Point trying to address? The answer, it appears, is a desire to defeat the seemingly unstoppable rise of bots. ▶

Did I just *send* that **file** to the ***wrong person?***

Check Point **DLP** prevents data breaches before they occur

Have you ever accidentally sent an email to the wrong person or attached a document that wasn't meant to be shared?

Check Point makes DLP work by combining technology and processes to move businesses from passive detection to prevention, before data breaches occur.

PREVENT data loss

EDUCATE users

ENFORCE data policies

HP Enterprise Security
www.bit.ly/hpcheckpoint

Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

"The statistics say that about 80% of spam today in the world is being delivered through the bot network.

We recently investigated a significant number of business attacks, and most of them are happening via bots – many of which are simply available for hire to criminals," he says.

"We decided to step in and help our customers. Our analyst teams looked at the command and control centres that these bots report back to. By tracking the communication of the bots, you can identify the bot, detect and quarantine the machine that the bot is using as a host into the enterprise.

To date, we've found bots in every environment where we installed and ran the software. This product is going to be very significant for us and our customers." he says.

That's just one of the challenges currently on the threat landscape and, like the rest of the industry, Amnon Bar-Lev is acutely aware of the challenges of BYOD and consumerization in the workplace, and again it is an area that Check Point is working hard to address. However, Bar-Lev is less concerned about the device and who provided it, as he explains.

"The device is not important. It's what I run on that device and how I enforce security on that device. That's the biggest issue, right?

Most of the people that use those devices insist on using the native applications like email and calendar but they don't want two architectures on the device: one for personal and one for business," he says.

"So we are trying to do two things. One is our Mobile Access Blade, which is, in effect, a VPN that allows a remote wipe of a stolen device and the ability to activate specific security controls on the device itself.

"The second is more exciting and will be delivered in the, I hope, not too distant future. Instead of just trying to protect the full device, what we need to do is to protect the data itself. So you can read mail on a native email application but the contents and attachments would all be secured," he says.

To help facilitate this, Check Point bought a company two years ago called Liquid Machines – a market leader for document security – and plans to integrate this technology both for mobile and non-mobile devices. Bar Lev also says that its Endpoint management solution is different from its rivals.

"We think it's unique because the issue with security management is not the device itself. What's secure about the policy is you as an individual. What is your role, what are your credentials, and what you do in the organization?" he says.

So does he believe that security hardware, including other companies, can keep pace with the rapidly-evolving and unpredictable trends such as social media and consumerization?

"It's tough, but in order to have better security, organizations need to run multiple security functionalities. And that means software. Check Point is purely a software company. We grew up as a software company and appliances are the packages that we bring to the market in order to help our customers – to make it much easier for them. You can come up with the security solutions very quickly when you are not tied purely to the hardware. You can upgrade the devices without necessarily dealing with the hardware itself," he says.

"For example, you can run Check Point in Amazon's Web Services environment with exactly with the same functionality as we have in each and every appliance. I think that's something unique to Check Point."

Bar Lev believes that because security vendors are driven by extreme pressures from the threat landscape the industry is much more innovative than others in the general IT field.

"Security is a space where you fight against somebody else – the hackers and the attackers, whoever and whatever they are. You need to respond to things that they generate as well. It's a never-ending challenge. It feels like that here at Check Point, the amount of innovative ideas, talent, energy and enthusiasm we put into that is huge. Look – we are a company of about 2,400 people and roughly almost 1,000 of them are in R&D," he says.

And as well as leading what is a very successful and continually growing business, Bar-Lev is still excited about just being in the security business and delivering to his customers.

"What's amazing about being in Check Point and in the security space, is that we have the opportunity to shape the industry and to shape the future of secure business practice. We are a market leader in our space and the fact that we can influence a substantial amount of businesses around the world, protect them and change the way they think about security and about the business is fascinating, really fascinating," he says.

"I do want my customers to be protected. I want them to do business. I do think it's making a better world for us, providing people with the opportunity to do whatever they want to do – in a safe manner and in an open environment," he says.

And that is a pretty good mission statement for anyone involved in security. ■

Digital Security as 'Corporate Social Responsibility'

The Information Security driver of Malaysia's very first Internet Service Provider, JARING Communications, has some recommendation for the guardians of digital security, specifically in the Asia Pacific and Japan region.

"I am afraid to say that, in terms of information security education and awareness, many industry players are guilty of not doing enough in this area and coordination is lacking across organizations, despite the fact that these activities can be considered as corporate social responsibility," said Raja Azrina Raja Othman, JARING's Head of information security and quality governance .

Based in Technology Park Malaysia, JARING (the name is based on the phrase 'Joint Advanced Research Integrated Networking') was formerly owned by MIMOS Berhad but, in December 2006, the Ministry of Finance of Malaysia officially took over the company.

"If we consider the numbers of Information Security Management System (ISMS) certified companies as a measure of the APJ take up rate, Japan is leading, with well beyond 400 certified companies, Taiwan also has more than 400 certified companies, South Korea more than 100, but Malaysia has only about 58 companies certified in ISMS," said Raja Azrina.

The ISMS standard was published by the International Organization for Standardization (ISO), which provided the above statistics, and the International Electrotechnical Commission (IEC) in October 2005. The system formally specifies a management system that is intended to bring information security under explicit management control and mandates specific requirements.

A security vehicle

"For organizations that realise that certification is not the ultimate aim, but more of a vehicle to carry the security agenda, they are more likely to succeed in maintaining security best practice within the organization," Raja Azina said. ▶

"When we take a look at the best approach to security – **'plan', 'do', 'check' and 'act'** – we need to realise that many organizations are not doing the 'check' thus a lot of exploits do not get under their radar," Raja Azrina said. "Many will only know there is a problem after the fact."

In her first job, this outspoken information security practitioner and digital security expert spent three years in JARING as a network engineer and system administrator for authentication and remote access servers. Back then she discovered a variety of security threats and worked on computer security issues on critical network devices.

A registered technical expert in information security under the the Department of Standards Malaysia, Raja Azrina has also been a representative on several of Malaysia's national level ICT security working groups formulating ICT Policies, including government security standard working groups.

After more than a decade, she is now back at JARING having been given the difficult task of ensuring information security is implemented and enforced, not only in back end processes, but also in service offerings.

Raja Azrina, who co-founded the Malaysian Computer Emergency Response Team (MyCERT), was formerly the CTO of a national agency. She has been involved in digital forensics since mid 90s, leading to the establishment of a Digital Forensics lab and services.

Top down or hard lesson

"Properly adopting data security best practice requires either a 'top down' push, or a hard lesson learned from an enterprise having fallen victim to attacks," she said. "The 'top down' push includes regulatory enforcement, promotional initiatives and incentives."

Raja Azrina said that the major challenge for data security in the Asia Pacific and Japan, and in all global regions, begins with governance, followed by technology, then measuring its effectiveness.

"Establishing and maintaining the metrics and measurement of security controls, should require a practical approach – less paper work – but more back-end intelligence and correlation processing, with consolidated reporting and compliance measurement," she said.

"Many organizations implement firewalls, intrusion prevention systems, intrusion detection systems, anti-virus programs; but never have the resources to review or properly analyse their logs.

Financiers and the military

As to the current dangers to information security and data, Raja Azrina believes that those whose critical infrastructure is under frequent threat are financial institutions and government enforcement bodies such as the military.

"Often the attack motivation is profiting from the confidential and sensitive information," she said. "It shows the value of certain information is far greater than the depreciated value of computer hardware hosting the information. And, despite the various sophisticated security measures in government military and security agencies, as well as financial institutions across the world, there are attackers who still manage to punch holes and exploit the slightest vulnerabilities."

Raja Azrina said that data security threats are very much common across borders, as long as the data resides on similar architecture and infrastructure.

Reviews of the main security threats for 2011 show malware as the most common threat to data security. In 2010, 'Stuxnet' was the beginning of targeted malware attacks and in 2011 'Zeus' started targeting Blackberry devices.

Collaboration with ISPs

DDoS attacks continue to be observed and appear to be on the rise in terms of frequency and Raja Azrina said these can be seasonal, for example, near to general elections. "Organizations need to understand that to mitigate DDos attacks effectively, requires collaboration with ISPs," she said.

"Phishing attacks are observed to be well orchestrated and to have well organized back end systems. To combat phishing requires an understanding of the life line for the phishing ecosystem. This requires cooperation from key players such as ICANN, internet domain registrars, CERTs and enforcement agencies."

There are growing concerns today among APJ organizations about the effect of 'social media' on trade secrets, productivity and privacy issues. Leaders also need to come to a view of whether social media is something that should be controlled and restricted versus leveraged and used for advantage.

"We see more organizations applying access restrictions to social media across their enterprise networks, but they are often lacking

in establishing well-defined policies to support this control," Raja Azrina said.

Vulnerabilities associated with online data remain in web application risks identified in the Open Web Application Security Project (OWASP) top 10, says Raja Azrina. (OWASP is a worldwide not-for-profit charitable organization focused on improving the security of software).

Software developers

"The top risk involves injection flaws in databases and directory servers," she said. "The root cause is primarily the web programming practice among software developers who need a greater understanding of security threats in order to build secure application and software.

"Software developers need to look at security the way engineers look at building a car; they embed safety into the design; they anticipate human error and mishaps. There are built-in warning and alert systems, yet you can't see the airbags. Never-the-less, they are there and they must function when needed.

"Security may not be transparent to users, but it must work and it must pre-empt human behaviour and bad practice. If this applies to what we call 'smart cars', then software applications need to be smart as well, in the context of data security," Raja Azrina said.

Some informed predictions about security threats over the coming few years have come from the SANS Technology Institute.

Raja Azrina said their insights include a forecast of more custom-targeted malware and zero-day attacks and hacking of mobile devices, which includes MITM (Man In The Middle attacks over Wi-Fi). There's also likely to be hacking of embedded or hardware-based systems as more devices go on the network, plus memory (or RAM) scraping threats. Some of these areas are actively being pursued in research in order to enable better understanding of preventive and defensive measures.

Ask hard questions

"What IT practitioners should do is to ensure that in their new solutions and technology evaluation process, they need to ask hard questions and demand a greater level of protection from these expected emerging threats," she said.

This pioneering information security practitioner said that the sophistication and complexity of today's multi-platform content delivery network and the spiralling range of human interface devices, has transformed the digital security game.

"I believe that any company offering interactive IT solutions must anticipate and prevent security threats from the early design stage of their solution," Raja Azrina said. "Security cannot be a piece meal of solutions. It must be integrated and seamless. Security may not be transparent to users, but it must work and it must pre-empt human behaviour and bad practice."

Raja Azrina has some firm views on the roles of specific IT practitioners in ensuring digital security.

She said the CIO has an important role in ensuring that investment made in data security controls is sustainable and provides business returns. The CIO also must ensure that sufficient resources are available for data protection. However, the type and basis of security technology selection and the effectiveness of security controls, "need to be advised by a savvy CISO".

"These two roles often have an adversarial relationship, but I call them 'sparring partners'," Raja Azrina said.

Recommended security strategy

This JARING Information Security Driver recommended a strategy for APJ organizations to adopt to ensure the best possible data security. She said some organizations believed that business continuity was the key factor. Others considered all aspects – preserving confidentiality, integrity and availability – as key success factors.

"Either way, a good strategy would be to comply with the established standards on information security, such as ISO 22301 Business Continuity Standard and ISO/IEC 27001:2005 ISMS," she said.

Raja Azrina said that security standards "will not tell you which product to buy, but will provide organizations with a comprehensive approach to security and indicate what elements of controls that need to be in place".

"It provides the approach, and the check list, to ensure organizations cover the breadth and depth of data security." ■

A secure approach to consumerization

The consumerization of IT has transcended theoretical discussion papers to become business reality. This presents both a challenge and an opportunity to global enterprises.

How can the CIO manage consumerization securely within their enterprise, with a view to maintaining business advantage as well as encouraging new working practices?

We tend to think of the consumerization of IT as a recent concept, but it was first discussed in a 2004 paper produced by the Leading Edge Forum. Even then the authors of the paper recognized the potential business benefits rather than the risks. The paper concluded:

"The 'consumerization' of information technology is a powerful trend that promises many significant long-term business consequences, including radically lower costs, greatly improved functionality, and successive generations of users who are ever more technology-savvy."

It's not a question of choosing consumerization or not – if enterprises wish to compete, they must adopt intelligent secure management of personal devices and behaviours in the workplace. For senior IT management, there is no avoiding what IT analysts, Gartner, describe as an 'irreversible mega trend'.

According to Gartner, global mobile device sales rose to 476.5 million units in the fourth quarter of 2011; a 5.4% increase from the same period in 2010.
In 2011 as a whole, there were 1.8 billion units sold, an 11.1% increase from 2010. Gartner also forecasts the overall market to grow another 7% in 2012, and smart phone growth of about 39%. Many of these smart phone purchases will end up in the enterprise.

In a separate study (Mobile Management Styles), Gartner estimated that smart phone sales had overtaken shipments of PCs in 2011. It said that global smart phone sales reached 461.5 million units and will increase to 645 million units in 2012. Additionally, the global number of downloads of mobile applications was predicted to total 18 billion applications in 2011 and set to rise to 31 billion applications in 2012.

Social trend watchers predict that 'millennials' (people born around 2000) will soon to enter the workplace and expect to use whatever application, device or technology they want.

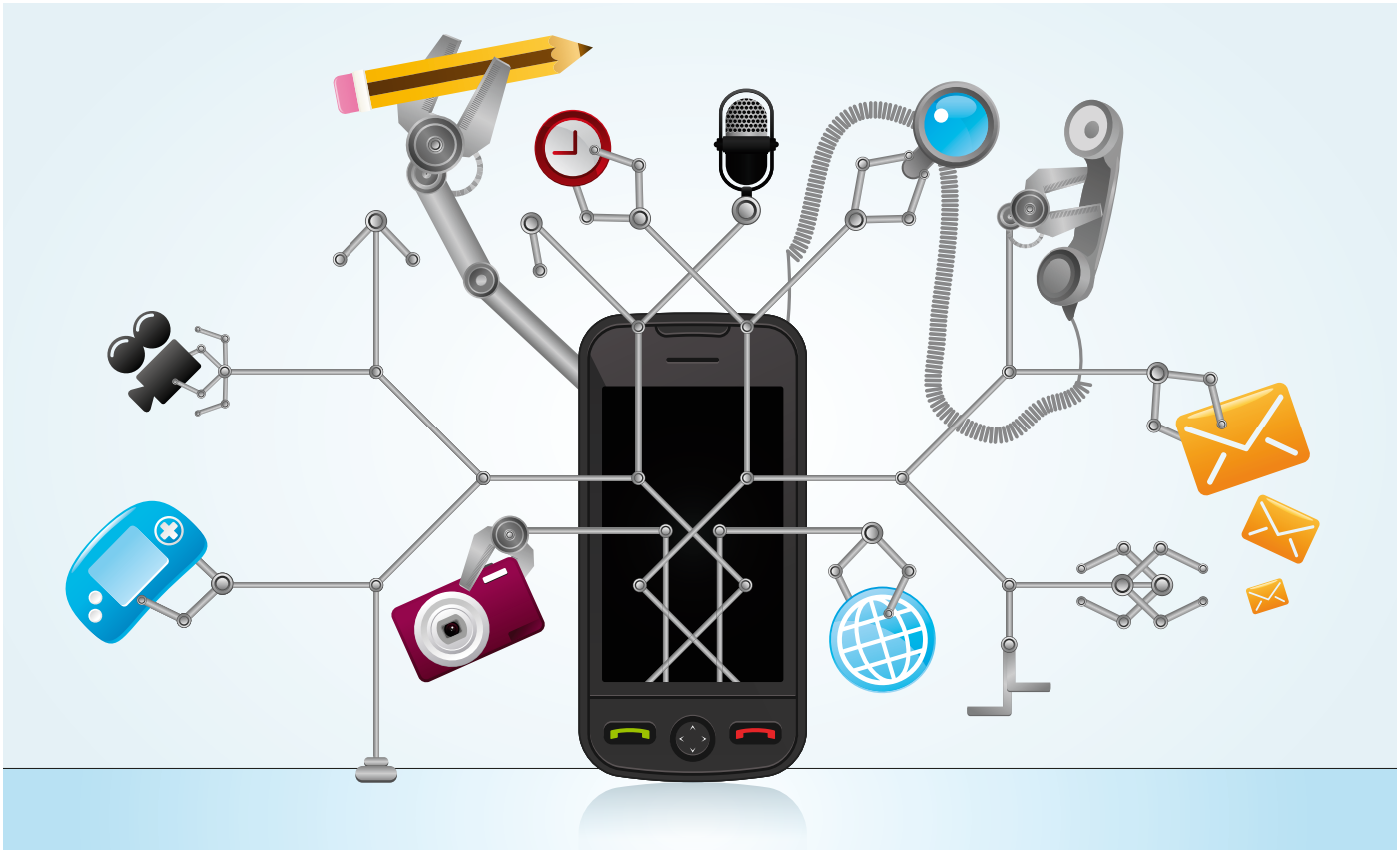
Mapping the use of personal devices in the workplace

Employees (acting as consumers) can purchase and set up personal technology, such as tablets and smart phones, which are more appealing in both functionality and technical specification than the IT equipment they receive from their employer.

This is unlikely to change as the dominant firms producing consumer devices (Apple, Microsoft, Google) are fully committed to frequent product refreshes as they play in a ferociously competitive market – particularly in smart phones.

Consumers and manufacturers are now locked in to a mutually beneficial ecosystem of rapid product change and development. For evidence, look no further than the product roadmap for Apple; people buy an iPhone knowing full well that a newer, better one will appear around 12 months later. Each launch brings new owners of iPhones attracted by the reputation of the existing model and millions more upgrading from that model. The same is now true of the iPad and rival smart consumer devices such as Android phones.

Recognizing that employees tend to be happier and, potentially, more productive with their technology of choice is a good first step along the road to managing consumerization. However, it is only a first step and managing all the aspects can become harder after that.



Four essential actions for consumerization

Assess

CIOs and CISOs need to assess the impact of consumerization on their enterprise bearing in mind many of the points listed above and take control of the situation.

A decision must be taken on how to manage personal devices based on sector, operations and working practices. In Gartner's words, they need to choose between orientations of control, choice, innovation or hands-off management approaches.

Transform

Consumerization is clearly a disruptive shift in technology ownership and processes in the workplace. It represents one of the biggest challenges for enterprise information managers for decades. Managed intelligently, it can serve the interests of employees and benefit the business.

Optimize

Security and IT policies must be revised to accommodate consumerization. This means developing a set of policies that define those devices, applications and working practices that will remain within existing corporate controls and those which can come under new consumerization policies and status.

Manage

This is crucial to successful adaptation of consumerization. CISOs and CIOs need to work with other parts of the business. This will include other C-suite members especially the CIO and the HR Director. Consumerization is a boardroom issue and strategies need top-level consultation and approval from the start. Information leaders must be at the forefront of managing consumerization as it pervades the entire organization. Other enterprise leaders will look to them for solutions.

Links and further references

This paper simplifies the risk assessment process through three fundamental principles. However to put these into practice you will need some practical help. Here are some useful resources:

Leading Edge Forum Consumerization paper (2004)	Good Technology State of BYOD report (2011)	Gartner Mobile Management Styles (2011)	How 4C thinking is the future for IT professionals (Paul Fisher 2011)	The invasion of the Smart Phones (Andrzej Kawalec, – HP 2011)	InfoSec 2011 McAfee Panel discussion paper (Paul Fisher 2011)
bit.ly/NdtmHv	**bit.ly/Nduk6C**	**bit.ly/KEan1z**	**bit.ly/KEapGM**	**bit.ly/LSZbjJ**	**bit.ly/KsHpZb** ■

SAFE NEVER SLEEPS™

Safe is advantage.
Safe is profit.
Safe is outright liberating.

But safe doesn't come easy.
Especially when the dark forces are plotting night and day.

It requires that delicate combination of brains and obsession.
A brutally effective, global team that can snuff out danger
before it gets dangerous.

That's McAfee, the world's largest dedicated security company.

We live and breathe digital security. Our job is to stay one step ahead.

We know that today real security isn't about "where," it's about everywhere.
Every device, every connection, every location, every second.

It's because we never sleep, that you can sleep better.

McAfee®
An Intel Company

www.mcafee.com/uk/safe

HP Enterprise Security Paras' 10 Team

On the 22nd March 2012, one of our colleagues gave birth to twins that arrived in this world much earlier than expected.

The twins are currently in the care of the Liverpool Women's Hospital where the situation has improved but they remain in a high dependence unit. It will be some time yet before their mother can take them home.

Liverpool Women's NHS Foundation Trust

It was through their mother that we learned of the incredible work carried out by Liverpool Women's Charity, providing direct support to parents with similar circumstances.

When one of your colleagues and friend needs the kind of help that you cannot provide, it becomes frustrating. An acceptance that family and experts are on hand to provide a higher level of support gives some comfort. On learning of the work of the charity, a small collection of friends and colleagues decided to do something to raise funds for the charity. The event chosen to bring awareness to the charity is The Parachute Regiment P Company Challenge "Paras10".

The Paras10 replicates one of the 8 tests required to be passed near the end of paratrooper training. It consists of a 10 mile cross country route, carrying a bergen (rucksack) weighing 35lb (excluding food water) and wearing long trousers with 'military style' boots. Competitor's rucksacks are weighed before and after the race, by race officials. The P Company Challenge is open to individuals and teams of 4 (with the first 3 runners to count). As a guide the Paratroopers Company Selection cut off time is 1 hr 50 minutes.

When it was announced generally to one of the HP offices, the response was outstanding. Within 24 hours the team had gone from 6 to over 20, and it currently stands at 28*. Some of these include friends of our colleague in the business and also other individuals from units within HP. Their backgrounds range from ex-forces to marathon runners to people who have never done anything even remotely like this. It is the latter that have already shown their determination to "get this done; often turning up before work at 07:00, to run through muddy fields, up and down hills, twice a week and in boots. Incredible 'espirit de corps.'

"For some this will be a return to an old stomping ground, for others it may just be the toughest thing they have ever attempted. The training and preparation is going to be hard, physically and mentally. Most are having to fit the training in and around a busy work/family schedule, but they are managing to do this. It will be an absolutely fantastic effort if all 28 get to the start line in September, and HP can be immensely proud of their colleagues when they cross that finish line." said Josh Randle, HP.

It will be an incredible journey for the team over the next few months, and the hope is that at the culmination of it all on the 9th September, the babies have come home.

Please Support us!

Please support us by donating at **www.justgiving.com/section20**

Follow our progress at **www.facebook.com/essparas10**

For more event detail visit www.paras10.com

***Meet the team:** Steve Aguirre, Ben Abraham, Dan Chaplin, Nick Cooper, Aileen Curran, Tony Elias, Kevan Ford, Antony John Gummery, Gary Hosken, Paul Hauxwell, Tony Higgs, Danny Hughes, Dave Jones, Matt Keay, Iain May, Mike McCarthy, Sarah McGowan, Dave McNab, Mike Pimlott, Steve Pinder, Karl Stoney, John Tipton, Craig Whilding, Simon Wildman, Tony Wilson, Rob Wood, Alison Wyatt and Bill Yoxall.

The SIEM advantage

Security Information and Event Management (SIEM) is fast becoming an essential tool for security professionals faced with an increasingly complex mixture of cyber threats, rapidly changing work patterns and increasing legislation.

The first SIEM products were introduced 10 years ago to solve a big data perimeter problem. Routers, firewalls and IDS tools were all generating a multitude of events that needed to be combined, filtered and turned into information. This made it possible for security operations staff to identify threats and then be able to respond to attacks.

Over time many products (including HP ArcSight SIEM) have expanded their capabilities to look across an ever expanding IT landscape. This landscape encompasses servers, databases, applications, vulnerability information and virus scan results, SCADA infrastructure, etc. Significantly, this also includes the people behind the actions. This process utilizes real-time collection; normalization and aggregation of log data from, potentially, thousands of sources. Advanced correlation processes are applied to identify suspicious patterns that could be specific to each individual business.

This is good news for the hard-pressed CISO or CIO whose world is getting more complex every day. It is obviously hard to maintain a reliable record of what is happening on networks and architecture – and it's getting harder all the time.

New ways of working in the enterprise – outsourcing, consumerization, virtualization, mobile and cloud – have resulted in a huge uplift in data calls and data transfers, driving additional log entries across the enterprise.

"SIEM is about consolidating and analyzing millions of security-related events coming from the logs generated by network devices and other security products to find and highlight actionable security incidents" Jay Huff, EMEA Director, HP Enterprise Security Products

Key challenges that SIEM can help with

It defends the organization against aggressive external threats including APTs: HP has been dealing with threats for profit (organized crime/nation state), but now also has to deal with threats that are more political or social in nature. Attacks are also targeted, persistent, well organized and happen over a period of time and below the radar.

- **Defend against malicious or compromised insiders, creating a bigger risk in increasingly tough financial climates**
- **Ensure that IT policies are adhered to and that supported products are functioning within normal parameters**
- **Assist in significantly automating compliance; reducing time and effort in preparing for audits**
- **Monitor and audit file downloads and data transfers**
- **Effectively identify and manage false positives**
- **Understand and effectively police configuration changes across the network**

The SIEM advantage

The new generation SIEM systems offer a unified state-of-the-network overview in an easy to understand dashboard display.

The best SIEM solutions can display a comprehensive, real-time overview of data flows and event logs recorded across the enterprise right out to the managed endpoints.

The i in SIEM

Some argue that it would be more accurate to attribute the "i" in SIEM to "intelligence", because the very best solutions offer a set of data that gives a valuable insight into the workings of the enterprise in terms of data flows and data efficiencies. It can be a valuable business as well as operational tool. Some ways in which SIEM offers more than just security are :

- Organize data for long term storage and meet compliance demands e.g. PCI-DSS
- Monitor employee server and data requests and flag suspicious or unusual activity
- Alert unauthorized configuration changes to servers and virtual machines
- Track specific application usage and bandwidth consumption levels for devices across the enterprise right out to the endpoint
- Determine real network breaches against false positives and deliver administrative efficiencies
- Ensure anti-virus and patches are up to date and functioning
- Generate error and breach reports and identify cause and system vulnerabilities
- Identify best efficiencies for third party security tools and improve ROI

Calculating ROI for SIEM

Making a business justification for investing in SIEM technology is often the hardest part of the security project. The value of security investments can be realized in the form of "soft benefits," such as increased situational awareness, reduced organizational risk, broader security visibility and better brand awareness – benefits that are hard to compute.

However, hard figures can often be calculated up front and verified over time. The business justification of a SIEM investment can be quantified by looking at cost break-even points, and the costs (or fines) avoided with the SIEM solution.

SIEM technology can help by removing inefficiencies through automation, avoiding infrastructure expansion costs, preventing expenditures for compliance penalties, reducing loss through fraud and minimising losses due to system outages.

By taking this approach, the security team is able to demonstrate the monetary value of SIEM investment, and align with business units to build a business case. There are several real-world examples of how organizations have seen quick break-even points, reduced their total cost of ownership and realized efficiencies with the help of their SIEM investment

Choosing the right SIEM for your business

While there are obvious business benefits to installing SIEM, it is not a magic box of tricks, nor a silver bullet to all business problems. "Often one of the main challenges in implementing a successful SIEM solution is that of scope management. The capabilities of any SIEM solution are, ultimately, only limited by the inputs available, tied in with the business logic that drives the reporting and alerts created by the system. Thus the participation of Project Management in addition to the business is fundamental to any SIEM project and its importance should not be underestimated." Chris Roberts, SIEM Practice Lead, HP Enterprise Security Services.

There are some additional caveats that you must bear in mind when considering SIEM:

- Think about your key objectives when implementing SIEM
- Compliance, data management, application management, security efficiency
- Ensure you have some basic analysis built into your solution
- A pile of logs on its own is worthless
- Train the right people to interpret the reporting output
- Meaningful actions based on log information
- Deploy scalable solutions
- Flexibility to change as your business needs develop

SIEM is much more than security. Think outside the "SIEM box" – work with your trusted security partner to tweak the SIEM to deliver real business intelligence to your enterprise.

In an age of data overload, a SIEM should make your life easier, not harder. ■

Videos: *Click to play*

What's new in ArcSight Logger with Hugh Njemanze, ArcSight CTO
http://bit.ly/LSVmLb

How HP ArcSight assisted Vodafone
http://bit.ly/M2b9Yy

Case studies:

Real-life examples on how SIEM delivered ROI and other efficiencies:
http://bit.ly/KT2iwu

How SIEM can deal with modern day threats:
http://bit.ly/L4wVx6

Q&A

You are an expert on risk. Do you think that CISOs still have yet to grasp the importance of risk assessment and risk management in their profession?

There really are no experts in risk management. When my company won the 1995 Information Security Program of the Year Award the Government Accountability Office came for a visit and asked us how we implemented security requirements. I told them that we didn't, we conducted a risk assessment to determine what threats posed the biggest risk and that we put our limited budget resources where they could do the most good. The CISO has its feet in two worlds, the technology world and the business world. An effective risk assessment program is cognizant of both and responds to both needs.

How important are security policies and procedures in enterprise security?

Without effectively implemented policies, standards and procedures there is no security program. In order to seek relief in the courts the company must show what steps they have taken to secure the assets of the enterprise. One way is through the written word. To be effective, policies and standard must be taken to the user community on a regular basis to keep the message in front of them.

Can policies and procedures keep pace with rapid technology shifts like consumerization and trends like big data?

Tier 1 or Global policies are written at a high level and are generally void of technology references. For example, there should be a Corporate Communication Policy that establishes what types of information is allowed in corporate correspondence and what information is prohibited. Then there should be a series of Tier 2 or Topic Specific policies that establish what users do when using the latest technology. When technology changes the Tier 2 policy changes but the Tier 1 policy continues to be appropriate.

Can you explain (briefly) the concepts behind your Facilitated Risk Analysis Process (FRAP) and why they are important?

The FRAP was created when we attempted to implement a risk assessment process and found that we had 4 hours to complete the process. The FRAP has evolved again during this past year to streamline the process even more. For example, from April through June of 2011, I conducted a FRAP for a state agency with 16 divisions. The FRAP lends itself to getting threats identified, risk levels established and compensating controls identified. In addition to the risk assessment process the new FRAP also has side benefits of identifying the applications, systems and business processes used by a department or division, what the criticality level is for each (Business Impact Analysis) and what information classification category each contain.

Are security awareness campaigns worth the trouble?

If they are conducted properly then yes. They can be used to raise awareness that threats exist. One method that seems to get the best results is to make the threat personal. That is show the user how this affects them at home and how we can help them combat that threat. Once the audience has internalized the issue they are more respective to controls introduced at work.

Which threat worries you the most?

Apathy.

"The CISO has its feet in two worlds, the technology world and the business world. An effective risk assessment program is cognizant of both and responds to both needs."

Thomas R. Peltier

The President of Thomas R. Peltier Associates, an information security training firm discusses risk and the impact of security policies on the enterprise.

What gives you the most satisfaction in your working day?

Helping a fellow security professional find an answer. We are all in this together and when one finds a solution we should share it with our peers.

How could security vendors do more to assist CISOs?

Understand that the CISO has his feet in two worlds and be sure the solution offered helps them meet the business objectives or mission of the enterprise. Security and audit requirements do not exist. There are business and mission requirements and legal and regulatory requirements. We never implement anything unless it supports the business or mission of the enterprise.

What would be one life lesson you would pass on to a college grad embarking on a career in information security?

Be willing to work to a compromise solution. Be willing to ask your peers for help. Take advantage of such organizations as ISSA and ISACA. These are your local support groups and they share solutions.

You've worked a lot in the car industry – is it a sector you are drawn to?

I did 22 years at GM and got my "parole" in 1992. From 1977 through today I have been in the information security profession. I live in the Detroit area and in 1970 the auto industry was the biggest employer in town.

Finally, how do you like to relax?

I enjoy taking walks with my wife and my dog Winston. ■

Symantec

Symantec white paper discusses DLP for tablet devices; webcast offers practical advice

As employee-owned tablets invade the corporate environment, CISO's need to support these new devices while managing data loss risk. A new Symantec white paper explores the options for securing confidential data on tablet devices and why data loss prevention should be considered.

An accompanying Symantec webcast explores the challenges of managing tablets in the enterprise and the security risks they pose. The webcast offers advice on tablets trends in the enterprise, how to monitor and protect sensitive data on iPads and an exclusive preview of Symantec Data Loss Prevention for Tablet.

White paper: http://bit.ly/L25Afz

Webcast: http://bit.ly/NcwNul

McAfee

New features on McAfee Network Security Platform impress NSS Labs

McAfee has announced several new capabilities to its Network Security Platform, including a scalable 80 Gbps IPS that has been validated at over twice the performance capability of other high capacity network IPS solutions available by experts at NSS.

"As organizations increase the capacity of their networks, we have seen an increase in the need for high throughput security solutions," says Vikram Phatak, CTO, NSS Labs.

"At NSS Labs we go to great lengths to determine the maximum performance a device can maintain under real world conditions. We put the McAfee Network Security Platform XC Cluster through our full network IPS test and it successfully passed over 72 Gbps of inspected traffic while maintaining an overall protection rating of 95%."

http://bit.ly/Kve7XI

Intel

New Intel security manual aimed at corporate executives.

Security has evolved from a tactical IT concern to boardroom-level dilemma. This transition has challenged many executives who are now obligated to protect their organization's critical assets. Security Battleground: An Executive Field Manual provides guidance to any executive who find themselves shouldering oversight responsibility for information security.

The Security Battleground team of authors designed this book to provide practical advice for security-obligated executives, that is, for business executives with or without formal backgrounds in security processes or technologies.

The lead author on the book is Mike Fey, SVP of Field Engineering and Advance Technology at Intel. The book is available direct from Intel and other online suppliers priced at $49.95.

http://intel.ly/JUv21c

McAfee

Management for optimized virtual environments delivers intelligent security

McAfee has unveiled a new agentless deployment option for its Management for Optimized Virtual Environments (MOVE) AV solution which it says, provides comprehensive defenses against all types of physical and virtual attacks through a single high performance console.

The solution has been designed to offer standardized security across all major hypervisors enabling security management and delivery for virtualized environments.

"McAfee MOVE AV provides McKesson with comprehensive and consistent malicious code protection for our virtual environment," said Patrick Enyart, Senior Director, McKesson Information Security, Security Operations.

"As we continue to adopt emerging technologies, particularly cloud computing solutions, implementing McAfee MOVE AV provides us with additional security in our virtual environment. The solution makes sizing and deployment simpler and ensures that every system is deployed with the same level of protection."

The company says that the MOVE AV agentless deployment option addresses the challenges of protecting virtual environments and keeping them free of malware without the bulk of an agent, resulting in easy deployment and set-up. Both deployment options (multi-platform and agentless) provide powerful, comprehensive, and consistent protection, and are managed and reported by the McAfee ePolicy Orchestrator platform.

http://bit.ly/KvdTzM

Social media vs the CISO

Social media is the phenomenon of our times with social, cultural and political impacts on society. It's also a headache for the CISO pressurized by peers to keep on top of the trend and find a way of securely harnessing the business benefits of Facebook and other social sites.

845m monthly active users

500m registered users

150m members

According to Wikipedia there are currently more than 200 social networking sites in existence around the world. As of December 2011 Facebook had 845 million monthly active users, with 483 million using the site every day. Meanwhile LinkedIn's 150m members generated 4.2 billion professionally-oriented searches on the platform in 2011.

Twitter has around 500 million registered users with 33 billion Tweets flying across the so-called "Twittersphere" every day. It's a good bet that most of your employees are members of more than one social media site.

At the same time, an increasing number of businesses see social media as an essential marketing and branding tool. Although aware of the brand implications from a data breach, marketing groups may not always prioritize security. Other employees happily updating social pages throughout the working day do not, as a rule, prioritize security.

Since October 2010, social networking usage patterns have become more active, with bandwidth consumption for Facebook Apps and posting increasing from 5 % (October 2010) to 25 % (December 2011) when measured as a percentage of total social networking bandwidth. Twitter browsing at work alone grew by more than 700 % year-over-year, according to Palo Alto networks.

Unfortunately for the CISO, the option to simply ban social media is a now a business dead end due to its overwhelming presence and its perceived benefits. The Harvard Business Review Analytics Services recently conducted a survey of 2,100 major organizations and discovered that 79% are currently using social media channels. The number one advantage, it discovered, was increased awareness of the organization.

The risks of social media

By now you know social media is embedded in your business and it isn't going to go away. Now you need to work out how to manage it securely and what the risks of social media are to your specific business and sector. A risk assessment exercise needs to be undertaken which must, at the very least, detail the likelihood and implications of the following:

- **Data loss via employee negligence through social media**
- **Data breach via social engineering through social media**
- **Malware or Trojan infection via social media download**
- **Brand damage after data leak**
- **Reputational failure via unregulated employee social media post**
- **Existing security policies not covering social media**

THINK SECURITY

The risks are very real. The Ponemon Institute has established that the per capita cost of a data breach is $194 ▶

Marketers

34% have generated leads using Twitter and 20% have closed deals

Consumers

56% more likely to recommend a brand after becoming a fan on Facebook

While according to compliance specialists Sailpoint,

1 in 5 adult Americans would stop doing business with a bank that suffers a breach while 10% of American adults would tell friends to stop doing business with a breached company.

Secure business advantages of social media

Having assessed the risks, consult with marketing, communications and HR teams to assess the business advantages and to ensure safe and risk-assessed usage of social media within the business for both personal and enterprise business usage. Social media has become a valuable, low-cost and effective marketing tool bringing customers closer.

The statistics back this up: 56% of consumers say they are more likely to recommend a brand after becoming a fan on Facebook, 34% of marketers have generated leads using Twitter. Meanwhile, 15% of 16-24 year olds prefer to receive customer service via social media over any other method, compared to just 8% of 25-34 year olds and 3% of those aged 35-44 according to media experts, Social Skinny.

As a security professional you cannot ignore the business message of these statistics, certainly the option of just blocking social media is no longer viable.

A recent Gartner study showed that in 2010, 50% of large organizations blocked social sites, but by 2014, that number will drop to 30%.

The study also found that for some company departments and processes, such as marketing, access to external social media is a business need. Meanwhile, employees are finding ways to circumvent corporate blocks by using their personal smart phones and other consumer devices.

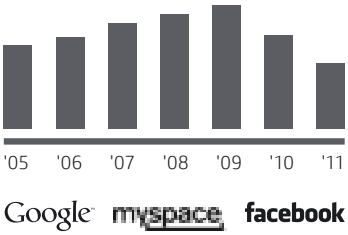
"Being social, even outside the confines of the company, make workers more comfortable and happy." Kevin Rice, Enterprise Network Architect, AT Kearney. (Computerworld)

Adapting or creating a Social Media Policy

Having conducted a social media risk assessment and consulted across the business from all social media stakeholders – including, let's not forget, your employees – it's time to formulate an enlightened and progressive, secure business focused Social Media Policy. This needs to be cleared by the board then explained and enforced to employees. Most importantly it needs to reflect the business and security needs of the enterprise – most of all taking into account all of the marketing and branding messages listed earlier.

No time to stand still

Social media is a fluid, disruptive and organic phenomenon subject to the whims of fashion and consumer habits. You need to keep an eye on emerging trends and which social media sites employees are using.



Google myspace facebook

Young people are particularly fickle as the fate of Myspace illustrates. From 2005 until early 2008, it was the most visited social networking site in the world. In April 2008 however, Facebook outstripped Myspace for unique worldwide visitors and unique US visitors in May 2009.

As of December 2011, Myspace was ranked 138th by total web traffic.

The point is that, unlike many conventional business driven security policies, social media needs the most constant attention and care as, not only do platforms and methods change, but also internal business departments will adapt their usage. There are also compliance and legal changes to think about. For example, the UK government wants to monitor the Internet use of every single citizen. Where is the corporate responsibility in that?

One solution to keeping social media secure is to appoint a social media champion as a trust agent in your risk or security team. ■

Security. It matters now more than ever.

Today's workforce takes care of business virtually any place, so you need the right security and risk management strategy firmly in place. Our end-to-end approach provides protection across your organization and the world.

visit us at
hp.com/enterprise/security

SYMANTEC IS SECURITY.

Solutions that protect the infrastructure, information, and interactions that drive the global economy.

SYMANTEC.COM/EVERYWHERE

Confidence in a connected world.

Symantec™