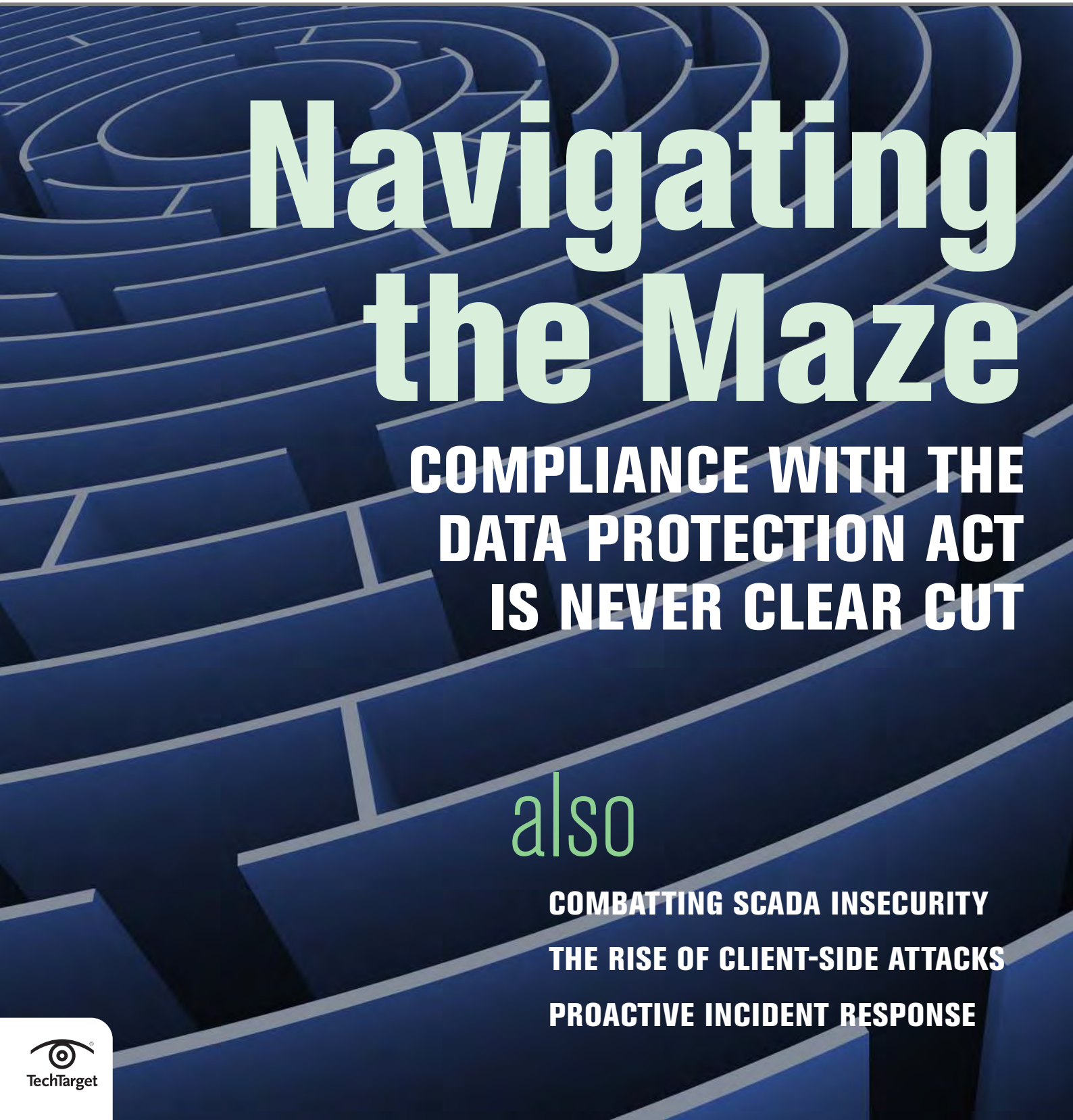
SUMMER 2011, VOLUME 1, NO. 2

IT in Europe

INFORMATION SECURITY EDITION

Special European edition of Information Security magazine | *www.SearchSecurity.co.UK*



Navigating the Maze

COMPLIANCE WITH THE DATA PROTECTION ACT IS NEVER CLEAR CUT

also

COMBATTING SCADA INSECURITY

THE RISE OF CLIENT-SIDE ATTACKS

PROACTIVE INCIDENT RESPONSE

TechTarget

Achieve Compliance. Securely.

Imperva, the Data Security leader, enables a complete security lifecycle to provide visibility and control for business databases and the applications that use them.

Thousands of the world's leading enterprises, government organizations, and managed service providers rely on Imperva SecureSphere to prevent sensitive data theft, protect against data breaches, secure applications, and ensure data confidentiality. Organizations across the globe use SecureSphere to reduce the cost and effort to comply with key industry regulations such as GLBA, PCI, and European Data Privacy Directives. SecureSphere's unmatched Data Security capabilities include:

- *Protection against SQL Injection and other sophisticated application-level attacks*
- *ICSA-certified Web application firewall*
- *Database vulnerability assessments and risk scoring*
- *100+ pre-defined and customized data compliance reports*
- *Enterprise-class protection against data breaches and attacks*

Whitepaper: Data Security and Compliance Lifecycle

Regulatory directives and compliance mandates are increasingly expanding formal enterprise audit processes to include information technology (IT) assets, especially databases. Imperva's Data Security and Compliance Lifecycle provides step-by-step best practices for implementing database controls and web application security.

Download the whitepaper here: www.imperva.com/go/sc

Imperva

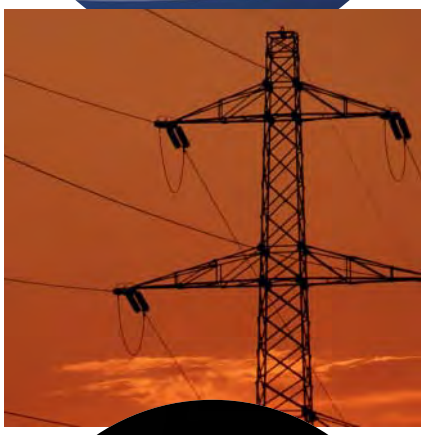
Visit us at: www.imperva.com or contact us at sales@imperva.com

SUMMER 2011, VOLUME 1, NO. 2

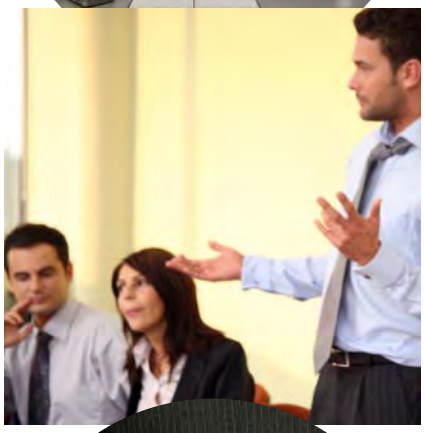
IT in Europe

INFORMATION SECURITY EDITION

FEATURES



DEPARTMENTS



Your One Stop Shop for All Things Security

Nowhere else will you find such a highly targeted combination of resources specifically dedicated to the success of today's IT-security professional. Free.

IT security pro's turn to the TechTarget Security Media Group for the information they require to keep their corporate data, systems and assets secure. We're the only information resource that provides immediate access to breaking industry news, virus alerts, new hacker threats and attacks, security standard compliance, videos, webcasts, white papers, podcasts, a selection of highly focused security newsletters and more — **all at no cost.**

Feature stories and analysis designed to meet the ever-changing need for information on security technologies and best practices.

INFORMATION SECURITY®

www.SearchSecurity.com

Breaking news, technical tips, security schools and more for enterprise IT professionals.

SearchSecurity.com

www.SearchSecurity.com

Learning materials geared towards ensuring security in high-risk financial environments.

SearchFinancialSecurity.com

www.SearchFinancialSecurity.com

UK-focused case studies and technical advice on the hottest topics in the UK Security industry.

SearchSecurity.co.UK

www.SearchSecurity.co.UK

Information Security strategies for the Midmarket IT professional.

SearchMidmarketSecurity.com

www.SearchMidmarketSecurity.com

Technical guidance AND business advice specialized for VARs, IT resellers and systems integrators.

SearchSecurityChannel.com

www.SearchSecurityChannel.com

TechTarget®
The IT Media ROI Experts

When Digital Risk Gets Physical: Assessing the Global Cyberthreat

The recent Kaspersky kidnapping serves to remind that threats to some information security pros involve more than stolen credit card details. BY RON CONDON

ON THE OPENING day of Infosecurity Europe 2011, when Eugene Kaspersky, founder of Kaspersky Labs, took the podium to deliver a wide-ranging and humorous speech about cybercriminals, he could hardly have imagined the news that would reach him shortly afterwards.

As we now know, his 20-year-old son Ivan had been kidnapped in Moscow and was being held for a ransom of 3 million euro. Kaspersky flew to Russia, and, with the help of security forces, managed to get his son freed without harm, and without paying any ransom.

Ironically, the theme of Kaspersky's talk had been "How to make the criminals unhappy," although he was obviously referring to cybercriminals, not kidnappers.

He said the last few years had been a golden age for cybercriminals; they have been able to make huge sums of money with little risk of ever being caught. But, he argued, the balance of power is now changing. Cloud-based reputation services, he said, enable antimalware companies to respond much faster to new threats, and thus limit the amount of damage hackers can cause.

That will, therefore, reduce the return on their investment, and make their activities less profitable. "I know from their comments that I see on underground forums that they are becoming very unhappy," he announced, grinning broadly.

Some types of malware, such as targeted attacks or server-side polymorphic malware, will still be able to bypass traditional defences and pose significant digital risk. But, as he said, that kind of code is much harder to write, and is beyond the skills of the majority of hackers.

He proposed a couple long-term solutions. The first was an Internet Interpol—a force capable of working internationally to catch criminals quickly that isn't subject to strong national boundaries that hamper current police investigations. The other is an Internet passport, a digital identifier that any individual would need to have before he or she could contribute information to the Internet.

Those measures, he predicted, might take 20 or even 30 years to achieve, but will be absolutely essential for generations of people who will expect to conduct most of their daily transactions online, whether it is voting in an election or arranging a social gathering. Such complete dependence, he said, will require the kinds of controls he proposed.

Meanwhile, the gang of unhappy criminals in Moscow who carried out the botched kidnapping is a reminder of the global cyberthreat that some of our best-known security researchers face in Russia and its neighbouring countries.

Mikko Hypponen, head of research at Finnish security company F-Secure Corp., admits that sometimes he has to moderate his public pronouncements because, as he says, when he drives to work in the morning he sees a sign reminding him that St. Petersburg is just a short drive across the border. The mafia there have a hand in all kinds of crime, including cybercrime, and so it would be unwise to antagonise them openly.

It's a sobering reminder that, while the worst that most of us can expect is to lose our credit card account details, some of those who play a critical role in defending cyberspace face much greater dangers.›

Ron Condon is UK bureau chief for SearchSecurity.co.UK. Send comments on this column to feedback@infosecuritymag.com.

DPA Policy

Data Protection Act compliance is—for better or worse—not a black and white process. BY ALAN CALDER

THE PROBLEM WITH the Data Protection Act, from a practical point of view, and in contrast to US-originated compliance standards like PCI DSS, is that the DPA does not contain a list of detailed, specific requirements that every organisation can decide are either applicable or not applicable, and, if they are applicable, tick off as having been complied with.

The problem with a tick box approach is that, where data security is concerned, one size definitely does not fit all. Threats evolve, and not all vulnerabilities are common. Compliance can be expensive and, if it is to be enforced, needs to be backed by an adequately resourced and aggressive regulator. The UK's ICO is neither adequately resourced nor aggressive. However, it will pounce on obvious negligence, particularly in the public sector. The trick with the DPA, therefore, is to keep out of trouble, not to look for a detailed compliance checklist.

Complying with the DPA is a process that can be broken down into three discrete stages. The first is simple: Do those things that the DPA specifically requires.

The DPA specifically mandates all organisations that intend to process personal data to:

1. Register as a Data Controller with the Information Commissioner's Office (ICO) (clause 18) with a description of the data the organisation will process.
2. Keep that notification up to date. Renew it annually and ensure the data processing description is still accurate.
3. Publish a 'Fair Processing Notice', which describes what data is being processed by the Data Controller (clause 7).
4. Operate a 'Subject Access Request' procedure (also clause 7), which enables any individual about whom data has been processed to have access to it, in order to find out what it is and/or to require it to be corrected or, under some circumstances, deleted.

Once those tasks are completed, the second phase of DPA compliance activity is about keeping out of trouble. Keeping out of trouble, in this context, means taking appropriate steps to protect personal data, in line with DPA Principle 7, and doing four specific things:

1. Ensuring all portable devices that could conceivably—under any circumstances—contain personal data are encrypted. This encryption has to be to a specific standard: FIPS 140-2. The loss of an unencrypted laptop, hard drive, USB stick, backup tape or CD that contains a selection of personal data will get the organisation in trouble. There will be press coverage and brand damage, upset individuals and, possibly, action by the ICO.
2. Ensuring websites that might contain personal data—irrespective of whether

they are e-commerce or straightforward information sites—are secure. At the very least, this means conducing penetration tests against all Web applications handling personal data and then taking the identified remediative steps necessary to secure those sites and applications.

3. Ensure network security is adequate. This means fixed networks should be subject to penetration testing, wireless networks should be WPA2 secured, there should be regular sweeps for rogue wireless access points and appropriate access control rules, and technologies should be in place, particularly for high-value personal data such as medical, religious, racial or similarly sensitive information.
4. Staff should be aware of their DPA responsibilities. This means key staff should have their DPA compliance responsibilities formally included in their job descriptions, the corporate disciplinary policy should allow for dismissal in cases where an individual breaches the DPA or the company's Data Protection Act policy, and all staff working with personal data should be subject to at least basic training in their DPA responsibilities. There are good e-learning packages available that enable corporations to apply a consistent level of training across the organisation and to maintain evidence as to which members of staff have successfully completed the required level of training.

You might think you've done enough to comply with the DPA once you've completed either the first or the second phases of activity described above. In fact, you will only have done enough to keep mostly out of trouble.

You might think you've done enough to comply with the DPA once you've completed either the first or the second phases of activity described above. In fact, you will only have done enough to keep mostly out of trouble.

You'll only know you've done enough to comply when you have identified all the personal data held within the organisation, carefully analysed all the risks to it (while ensuring you have adequate measures in place to keep the data current and for no longer than required) and rolled out controls to reduce those risks to a minimal level.

While organisations might find this approach more challenging, it is more likely to protect personal data than one that relies entirely on a standardised list of controls; information security risks mutate and evolve more quickly, and effective defences against data breaches have to be similarly alert. This is, of course, the core premise of ISO/IEC 27001, the best practice information security management standard. However, compliance with ISO 27001 is not, on its own, enough. For example, Epsilon, which was recently subject to a massive data breach, is ISO27001 compliant.

Compliance of virtually all sorts is a nuanced pursuit: Every day that you avoid a data breach, you will have done enough to comply with the DPA; on the day you suffer

a breach, you will not have done enough. Intelligent risk mitigation is about identifying those possibilities and eliminating them before they are exploited. From the data subject's point of view, this is a far better approach than one that allows his or her data to be stolen, but excuses the custodian because it had ticked all the boxes.›

Alan Calder is a leading author on information security and IT governance issues. He is also chief executive of IT Governance Limited, the one-stop-shop for books, tools, information and advice on governance, risk management and compliance in the UK. Alan was previously CEO of Wide Learning, a supplier of e-learning; of Focus Central London, a training and enterprise council; and of Business Link London City Partners, a government agency focused on helping growing businesses to develop. He was a member of the Information Age Competitiveness Working Group of the UK Government's Department for Trade & Industry, and is a member of the DNV Certification Services Certification Committee, which certifies compliance with international standards including BS7799.

ANALYSIS | EMERGING THREATS

Information Security Vendors Lag Threat Vectors

Products to secure smartphones and cloud computing are in short supply. BY RON CONDON

AS A SNAPSHOT of the state of our industry, the Infosecurity Europe conference in April underlined the extraordinary pace of change that enterprises are facing.

In 2010, the security implications of smartphones and cloud computing were just coming on the agenda; a year later, these threat vectors took centre stage. Successive debates and panel discussions at this year's conference revealed a growing concern over these twin trends that apparently seem unstoppable since cloud computing is cheap, and smartphones are sexy.

In both cases, it seems organisations are falling over themselves to adopt these technologies without letting security considerations get in the way.

The economics of cloud computing make it hard to resist, especially for companies struggling to cope with the long recession. As many Infosec exhibitors reported, organisations are desperate to reduce both their capital expenditure and their operational overheads. Cloud services can fulfil both those aims, and they may even improve security by applying a level of discipline and professionalism that organisations would struggle to achieve on their own.

In the case of smartphones and tablets, demand is fuelled by senior managers who buy good looking products, such as the Apple iPad, and demand to have them connected to the corporate network. Again, the general consensus from CISOs involved in conference discussions was that, if the boss wants an iPad, then IT has to find a way to make it happen.

However, both phenomena have security pros scratching their heads on how to minimise the risks. Some technological solutions were on display, mainly antivirus products adapted for smartphone platforms, but, on the whole, the industry is still looking for answers.

The biggest question mark hanging over cloud services is: How can an organisation know the provider will protect its data? A service-level agreement does not guarantee or verify security policies are followed to the letter.

Some kind of auditing regime is required, but the cloud providers rightly argue they cannot be expected to let every customer do an audit. Some professional bodies, notably the Cloud Security Alliance, have come up with a standard questionnaire to ease the process. But, as several CISOs reported from personal experience, the cloud service providers have so much business at the moment that they can afford to say, "Take it or leave it" to prospective clients. They will not answer questionnaires, asserting their security is fine: Just take their word for it.

Some companies accept those assurances at face value. But, as the recent breaches at RSA, Epsilon and Sony have shown, big systems holding valuable data, no matter how well defended, will always act as a magnet for the criminally inclined. And, a big cloud service provider would certainly fall into that category.

Under the circumstances, information security professionals said they are trying to confine the use of the cloud to non-sensitive data. Regulatory compliance may also limit its use, especially if the service provider cannot guarantee personal data will stay within the EU. Even cost cutting bosses want to stay inside the law.

Some kind of auditing regime is required, but the cloud providers rightly argue they cannot be expected to let every customer do an audit.

In the case of smartphones, security professionals are also focusing on risk limitation. Several CISOs seemed relaxed about allowing iPhones and iPads because of Apple's 'walled garden' approach to its App Store. The reliability of the apps, plus some of the features built into the IOS operating system, have persuaded many that Apple devices can be accommodated alongside the more traditionally accepted BlackBerry. But, most draw the line at giving network connections to Android, which they see as an uncontrollable and dangerous device that may harbour malware.

SECURING WEB 2.0

While users pondered how to handle upcoming problems, security vendors have finally caught up with a problem first raised two or three years ago: What to do about Web 2.0 and social networking applications?

As with the cloud and smartphones, a sudden wave of demand from employees and businesses presented security personnel with a huge challenge. Outright blocking was unpopular and difficult to achieve, and few firewall vendors were able to distinguish between harmless HTTP traffic (Web access) and other Web-based applications, such as Facebook, Twitter or Skype.

Furthermore, companies needed to regulate who used what aspects of social networking. For instance, they might permit Facebook, but not the uploading of sensitive

files, or they might allow Skype phone calls and instant messaging, but not the sending of attachments.

That level of granular control has been hard to come by. For a while, Palo Alto Networks had the application-aware firewall space to itself, although its pricing excluded all but the larger organisations. Over time, however, other manufacturers have updated their products. At Infosec, firewall manufacturer Watchguard announced support for application control, and SonicWall introduced similar features on its UTM appliances, with even more granular control to come later in the year. Sourcefire, a maker of intrusion prevention systems, also announced greater application control in its systems. Those announcements and others will allow smaller organisations to finally regain control over Web 2.0 applications, which are increasingly being used by hackers to deliver malware.

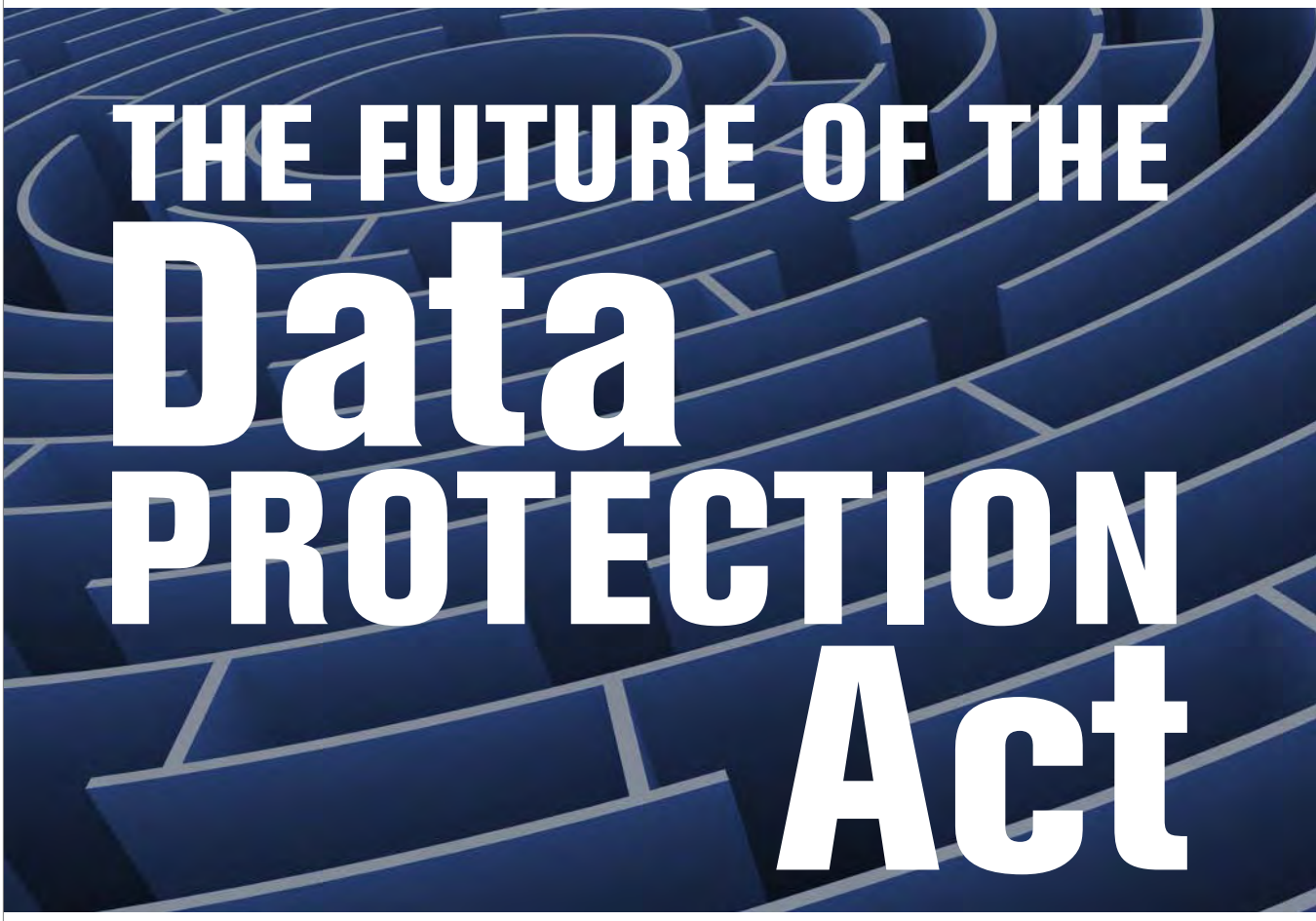
DEATH OF THE PASSWORD?

Some problems in security never change, one of the most enduring being what to do about passwords. The well-publicised breach of the system supporting RSA's SecurID one-time password infrastructure, just a couple of weeks before Infosecurity, provided rival vendors of two-factor authentication with a rare opportunity to promote their products as an urgent and viable alternative.

A string of information security vendors, including Swivel, GridSure, Signify, SecurEnvoy, CryptoCard and Winfrasoft, promoted a range of products with and without tokens. Some relied on delivering a simple code while others used a pattern-based method to deliver one-time codes. Most reported brisk interest on their exhibition stands, but whether that turns into business is another matter.

Thus, as continues to be the case, reports of the death of the password may be a little premature.›

Ron Condon is UK bureau chief for SearchSecurity.co.UK. Send comments on this column to feedback@infosecuritymag.com.



THE FUTURE OF THE Data PROTECTION Act

CAN ORGANISATIONS EXPECT A MORE PRESCRIPTIVE DATA PROTECTION ACT IN THE FUTURE? UK BUREAU CHIEF RON CONDON EXAMINES THE LAW'S PROSPECTS.

FOR A PIECE of legislation that first hit the statute book in 1984, the Data Protection Act (DPA) has weathered remarkably well. By sticking to broad principles and avoiding any reference to specific technologies from the start, it has managed to stay relevant for nearly 30 years, despite huge social and technological changes.

The underlying guidelines, embodied in eight simple principles, are easy to understand and remain a model of clear-sighted lawmaking. Although it was updated in 1998 to bring it into line with EU legislation (which it had influenced), the act has remained essentially the same.

So why has the act caused so much confusion and been the subject of so much misinterpretation over the years? Some organisations appear to use it as a convenient veil to avoid releasing any information at all, while others still treat personal information with reckless abandon.

Even the police got it wrong, most notably in the Soham murders investigation of

2002 where an overly strict interpretation of the act's requirements caused vital information to be missed.

Part of the problem lies in the principles-based approach, which leaves DPA compliance open to interpretation. Unlike other compliance regimes, it is not a regulation for which an organisation can tick all the boxes and declare itself safe.

"The principles are written in a way that they can be applied equally across a range of organisations, from a major bank or government department to a local corner shop," said Phil Jones, a former assistant commissioner with the Information Commissioner's Office (ICO), and now a consultant with the Promontory Finance Group LLC. "The trick is that they have to be applied and interpreted in context. If you get stuck, just behave decently—treat other people's information in a way you'd like your own information to be treated."

"The principles are written in a way that they can be applied equally across a range of organisations, from a major bank or government department to a local corner shop."

–PHIL JONES, former assistant commissioner with the Information Commissioner's Office

That is a good guiding principle, but doing the decent thing will only take you so far. For most organisations, data protection is complicated by a whole range of other factors—from operating in different countries with different laws, to outsourcing and using new technologies, such as social networking and geo-location. All these factors add new dimensions and raise new questions about exactly what is required by the law.

Help is at hand, of course. The ICO, for all its new powers to punish, is primarily motivated to encourage and enable good practice. Its website carries a fund of advice and guidance, both on how to protect data and what to do in case of a breach. There is also no shortage of consultants willing to take companies through the rules.

The soft approach appears to be bearing fruit. In a recent speech at the 2011 Infosecurity conference in London, Deputy Information Commissioner David Smith said that, although breaches still occur, few are in the same league as big breaches of the recent past—the lost CDs at HMRC, the loss of an MoD laptop containing details of army recruits, and the loss of 84,000 prisoner records by PA Consulting—which were marked by a lack of care and poorly defined responsibilities.

Those events, plus some breaches at financial institutions that drew heavy fines by the Financial Services Authority, appear to have marked a turning point in how we view data protection. Before those breaches, the DPA was a bit of an irrelevance; since then, the public sector has been given a huge shake-up as part of the government's Data Handling Review, and the ICO has been granted new powers to levy fines of up to £500,000 for serious breaches.

With these developments has come a broader awareness of the law across industry and the public sector, and a new-found respect for the ICO. Once regarded as a paper tiger, its new powers have made it a force to be reckoned with.

Any data loss in the public sector now has to be reported, and (for the moment at least) a regime of voluntary disclosure operates in the private sector. According to Smith, the ICO has received around 1,500 breach notifications since Nov 2007, and, in the year ending March 2011, 186 came from the private sector, 165 from health authorities and 146 from local government.

Although the ICO has had the power to levy fines since April 2010, only four fines have been handed out so far, three of them against local authorities, and all well below the £500,000 maximum.

In most cases, however, the ICO has taken a more lenient line, allowing the organisations in question to make a public statement of guilt, and commence an undertaking to rectify their operating methods in order to avoid a future breach.

DATA PROTECTION ACT CHANGES

The next major changes in the DPA regime come into place in May with an extension of the Privacy and Electronic Communications Regulations (PECR), which govern how companies carry out marketing campaigns.

Included in the changes is a new obligation on telecommunications companies and Internet service providers (ISPs) to disclose serious data breaches, and some new mandatory auditing rights for the ICO.

But, the aspect that is likely to affect most companies applies to the use of cookies on websites. The new rules say that organisations should seek explicit consent from site visitors to use cookies, and they should explain what the cookies do. For most companies, this will come as a bit of a surprise, and, so far, there is no guidance from the ICO on how the new rules should be implemented, although guidance has been promised.

Calder predicts a few organisations will try to implement it, while the rest will ignore it on the basis that most consumers don't understand cookies anyway and will not notice.

Under the circumstances, Smith said, the ICO will take a relaxed approach to the new rules, at least in the short term, to allow companies to make any changes they need.

Some experts have greeted this new regulation with scepticism, bordering on derision. Alan Calder, managing director of IT Governance Ltd, described the law as "unworkable" and said that, where authorities in other EU countries have tried to introduce it, they have met with "huge anger from advertising companies and Web commerce companies."

Calder predicts a few organisations will try to implement it, while the rest will ignore it on the basis that most consumers don't understand cookies anyway and will not notice.

Chris Barling, CEO of Actinic Ltd, which supplies e-commerce website software to small companies, was even more scathing. "I've generally been pro the EU over the years, but the sheer stupidity of the latest ruling on cookies has left me breathless. It's

hard enough already for small companies to compete when selling online, but this will make it even harder," he said. "The impact of this ruling will be to increase confusion and reduce choice. The chaos that ensues is likely to make it harder to protect privacy."

Nonetheless, the European Commission is pushing along with yet more plans for stronger data protection laws. In November 2010 it issued a communication—"a comprehensive approach on personal data protection in the European Union" (.pdf)—wherein it outlined plans to update its 1995 Data Protection Directive to take account of new technological changes and an increasingly globalised world.

It is a broad-ranging document, but buried in the text is a clear indication that mandatory disclosure for all breaches is on the agenda. "The Commission will examine the modalities for extending the obligation to notify personal data breaches to other sectors," it says.

Smith believes that broader obligation could be in law within the next three years, although he said it should only apply to serious breaches where damage could occur to individuals.

The Commission will pursue the idea of "the right to be forgotten," so individuals can have all record of themselves removed (with notable exceptions, such a prison records) if they so wish.

"I am in favour of a universal breach declaration requirement. You need compulsion to get organisations to pay attention to data protection."

––ALAN CALDER, managing director, IT Governance Ltd.

Most experts welcome the move to mandatory breach disclosure, mainly because it will force companies to take data protection more seriously. "I am in favour of a universal breach declaration requirement," said Alan Calder. "You need compulsion to get organisations to pay attention to data protection. Take the recent Sony breach, for instance. If there were a breach law saying you had to own up in 24 hours and inform customers, then Sony would be in serious trouble. Companies will have to put in place procedures for telling people of a breach. Then maybe they'll make more of an effort to protect data."

George Thompson, a director at KPMG, also believes mandatory disclosure will be of benefit and should be included in Data Protection Act guidelines. He said that, with few exceptions, many companies still go through the motions of having a data protection policy and appointing a chief privacy officer, but they fail to connect the policy with procedures and controls in any meaningful way. "Some organisations are mature, and have privacy and management systems, but not many," he said. "Mandatory disclosure would be a good thing, not least because organisations will need to work out how to respond should a breach occur. We've seen examples where the time taken to notify has been excessive, and the quality of information provided to customers has been quite poor."

Thompson goes even further, and suggests that a more prescriptive regime—along the lines of the US-based Sarbanes-Oxley Act—could be applied to personal information. "Sarbanes-Oxley is fairly prescriptive about the controls you need in place to protect the

LESSONS LEARNED FROM EARLIER BREACHES

The ICO recognises that accidents will happen, and that security can never be absolute. The best any organisation can do is to take all appropriate steps to protect personal data in its care. If a breach occurs despite the company's best efforts, and the company can prove it took appropriate measures and had proper procedures in place, then it has a good chance of avoiding punishment.

But, as Deputy Information Commissioner David Smith explained, some of the lessons from earlier breaches indicate just how easy it is for companies to lose focus and suffer a breach. Smith gave the following examples:

DATA RETENTION

The DPA stipulates a company should only store the information it needs, and only for as long as it is needed. Companies therefore need to focus more on weeding out old and redundant data. The less companies keep, the less chance they have of losing it.

TRAINING AND AWARENESS

Getting employees to sign a policy is not enough. Security needs to become part of everyday business, with staff fully conversant with the reasons why security is important. Policies and procedures also need to be related to the jobs that people do.

OUTSOURCING

Responsibility for security cannot be outsourced, so organisations need to monitor and check the state of information security at their contractors, outsourcers and offshore processors.

DON'T FORGET FAX AND EMAIL

One of the fines handed out by the ICO was against a local authority that faxed sensitive personal details to the wrong number. Email messages can also go to the wrong recipient, particularly when the user types in the first few characters of the intended recipient's name and the email software offers a list of potential candidates. Unless the user is alert, it is easy to click on the wrong name.

SHARED SERVICES

In projects where a number of users (possibly some in other companies) share information, the potential risks need to be assessed and controls put in place.

MOVERS AND LEAVERS

Have policies to ensure users only have rights associated with their jobs, and do not accumulate rights as they move around an organisation. When people leave the organisation, have a process to ensure they lose access to systems.

KEEP TABS ON PHYSICAL SECURITY

An unmonitored intruder can look at papers and screens, and even steal documents and computer hardware.›

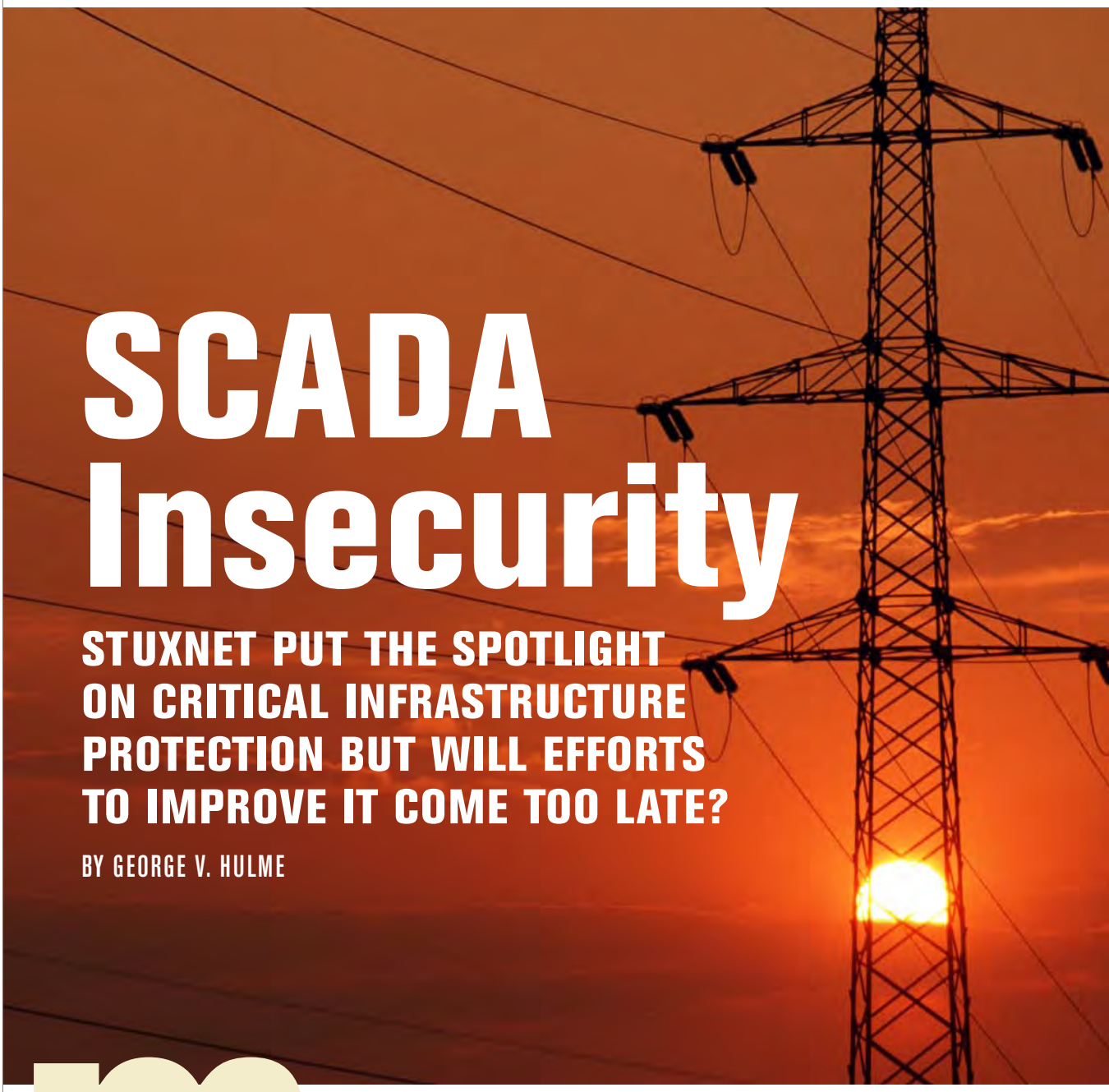
–RON CONDON

integrity of the financial statement. If we had something similar that covered confidentiality of customer data and external audit in the same way as Sarbanes-Oxley, that would be a big driver for organisations."

Some others suggest that the Payment Card Industry Data Security Standard (PCI DSS) could be extended to cover personal information, so organisations would be obliged to get themselves audited and certified compliant. A couple of American states have already taken that route.

But Calder is a strong defender of the DPA in its current form. "One of the weaknesses of detailed tick-box legislation is that one size doesn't fit all," he said. "The fact that you've ticked all the boxes doesn't necessarily mean you've set out to protect information properly. Threats change so quickly. The principles-based approach, while difficult at one level because it's not obvious when you've complied, is better because it forces you into a continual evaluation of risk and appropriate mitigation."

Ron Condon is UK bureau chief for SearchSecurity.co.UK. Send comments on this column to feedback@infosecuritymag.com.



SCADA Insecurity

STUXNET PUT THE SPOTLIGHT ON CRITICAL INFRASTRUCTURE PROTECTION BUT WILL EFFORTS TO IMPROVE IT COME TOO LATE?

BY GEORGE V. HULME

MARK WEATHERFORD will likely not forget the week of July 12, 2010. He'd just started his job as vice president and chief security officer at the North American Electric Reliability Corporation (NERC) that week. And, as chance would have it, security researchers had recently announced the discovery of Stuxnet, one of the most advanced worms on record and widely believed to be targeting Iranian nuclear facilities. With NERC's mission being to ensure the reliability of the North American bulk power system, it was a leap right into the fire for Weatherford.

The Windows-based worm, which contained a programmable logic controller (PLC) root kit, is the first known worm that can reprogramme industrial systems, and was crafted to breach Supervisory Control And Data Acquisition (SCADA) systems. SCADA systems are often used to control and monitor industrial processes, including those that help to manage power grids.

Immediately, Weatherford put into place a "Malware Tiger Team" that could be leveraged to help NERC ensure that the information about Stuxnet that was shared among facilities was accurate and useful. The team was comprised of malware experts and representatives from a number of federal agencies. Once the initial commotion over Stuxnet subsided, the team's role faded, but not its ability to reconvene quickly should another threat against the power generation and distribution system materialise.

While the hope is that such a need never arises, the probabilities point to someday in the future when the Tiger Team is called back to work. The extremely sophisticated Stuxnet worm highlighted the vulnerability of the critical infrastructure the world relies on, and security experts worry it could be a harbinger of future attacks. That's especially true as nation-states increasingly invest in their offensive cyberattack capabilities. Just as concerning as the threat, experts say, is that efforts to secure the SCADA systems used to manage many of the critical systems for controlling electricity, water delivery and other essential services have been lax. The federal government and industry groups are taking steps to secure the grid and the SCADA systems that support it, but many worry time is running out before a significant attack hits.

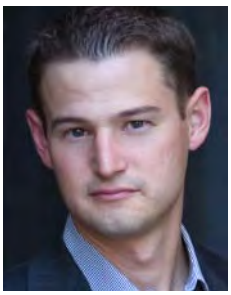
The extremely sophisticated Stuxnet worm highlighted the vulnerability of the critical infrastructure the world relies on, and security experts worry it could be a harbinger of future attacks.

RISING THREATS

There's no question that concern over critical infrastructure security is growing. Consider the findings in a report released last year by the Center for Strategic and International Studies (CSIS), and funded by security firm McAfee, *In the Crossfire: Critical Infrastructure in the Age of Cyberwar*. Based on a survey of 600 IT security managers from critical infrastructure organisations, the report found that 37 percent believed the vulnerability of the sector they worked in increased over the year prior, and two-fifths expect a significant security incident in their sector in the next year. Only one-fifth of respondents to the survey believe their sector to be safe from serious cyberattack in the next five years.

While there was no devastating attack that hit the IT systems that support the North American critical infrastructure, 2010 will nonetheless go down as a decisive year for malware and digital attacks. Cybercriminals (who themselves edged-out the hacker-hobbyist years ago) took a backseat to the state-sponsored attacker. These attackers are well trained, well funded, and professional. They pose perhaps the greatest threat we've yet to see face the critical infrastructure. In fact, the CSIS survey found 60 percent of those surveyed believe foreign governments have been involved in past infrastructure infiltrations.

Researchers at Moscow, Russia-based Kaspersky Lab, where two of the four zero-day vulnerabilities the Stuxnet worm exploited were identified, reported that Stuxnet's mission was to infiltrate a specific industrial control system that both monitors and controls industrial, infrastructure, and many on-site processes. It certainly wasn't considered an amateur job. "The inside knowledge of SCADA technology, the sophistication of the multi-layered attack, the use of multiple zero-day vulnerabilities and legitimate certificates bring us to an understanding that Stuxnet was created by a team of extremely skilled professionals who possessed vast resources and financial support," the company said in a bulletin.



"I view Stuxnet as a weapons delivery system, like the B-2 bomber."

–MICHAEL ASSANTE, president and CEO, National Board of Information Security Examiners, and former vice president and chief security officer at NERC and critical infrastructure protection strategist at Idaho National Lab

"I view Stuxnet as a weapons delivery system, like the B-2 bomber," says Michael Assante, president and CEO at the National Board of Information Security Examiners, and former vice president and chief security officer at NERC and critical infrastructure protection strategist at Idaho National Lab. "The code was designed to be very modular, so that its attack payload could be changed to be able to attack different systems. It's clear to me that the resources available to the authors of the worm were substantial. They designed it with high confidence that the warhead would do exactly what it was designed to do," Assante says. "That takes skill and resources."

That combination of well-heeled attackers and sophisticated malware means the stakes are much higher today than a few years ago when it comes to securing the critical infrastructure. This rise in the capabilities of cyber adversaries should be of concern to everyone. Civilisation is dependent on the critical systems that control electricity, finances, communications, water delivery, food distribution, and manufacturing. And the management of many those systems themselves are largely dependent on SCADA systems. Years ago, however, when these SCADA systems were first developed, they weren't designed to be resilient to today's security threats or heavy reliance on common and commercially available software applications, operating systems or for communications over public networks such as the Internet.

IGNORING THE RISKS

As SCADA systems have become increasingly networked, many believe that the industry and the federal government have not taken strong enough steps to ensure these systems are secure. "The industries that ignored cybersecurity, regardless of what the government said, are still doing just that," says Alan Paller, director of research at the SANS Institute. "It's a fundamental market failure. The industry said it would take care of things, and it didn't do the job it said it would do."

Others agree. "As long as there have not been any attacks [on their critical systems], it's hard for [insiders] to argue to make something more secure," says Richard Stiennon, chief research analyst at IT Harvest and author of *Surviving Cyberwar*. "There were no attacks last year, and there probably won't be attacks next year. So we're not spending on security because you say we should," is the typical response security professionals hear from their management, Stiennon says.

"Following Stuxnet, one would think that there would have been a surge of activity to protect the grid, but there wasn't," Paller says.

That apathy extends to the developers of industrial control systems, others say. "There is this climate where everyone understands the potential for mischief, but no one is talking openly about it. And the people who are finding vulnerabilities in SCADA systems and report them to the vendors find themselves in an adversarial situation," says Shawn Moyer, principal consultant at FishNet Security, who co-presented a session on "Wardriving the Smart Grid" at BlackHat 2010. "What is going on in this industry today seems a lot like what was going on in the IT industry in the late 1990s when most software companies simply ignored security."

"Following Stuxnet, one would think that there would have been a surge of activity to protect the grid, but there wasn't."

–ALAN PALLER, director of research at the SANS Institute

"When it comes to SCADA vendors, we are really early in the maturity curve," agrees Assante. For instance, he says, while security administrators at critical infrastructure organisations would like to know how to best harden those systems, the vendors don't always provide the necessary documentation that explains how to do so.

"The vendors understand that security matters, and they're starting to work security into their development processes. Generally, however, their security engineers probably aren't part of the developments teams," he says. "Security is not built into their processes. Over the next couple years, critical infrastructure vendors are going to have to more tightly integrate security into their design and product support initiatives," he says.

REGULATIONS IN THE WORKS

The federal government and industry groups aren't standing still when it comes to securing the grid and SCADA-dependent systems. And they're helping guide the way to more secure and sustainable power systems. Last June, the Department of Homeland Security (DHS) released its Catalog of Control Systems Security Recommendations for Standards Developers that aims to help facilitate the creation of security standards for SCADA, process control, distributed control, and other critical infrastructure systems. The standards help to detail everything from how such industries

can screen personnel to establishing physical security and setting secure configuration management guidelines. NERC, for its part, maintains security standards and guidance to roughly 2,000 public and private firms involved in electricity production and distribution in North America.

NERC's Critical Infrastructure Protection (CIP) regulations were designed to help ensure the reliability of bulk power generation and delivery. NERC CIP regulations comprise eight mandatory requirements that establish the minimum acceptable level of risk, and include security log collection and analysis, access control, reporting, intrusion detection/prevention system, among others. "The standards have only been auditable for a couple of years, and we are light years improved from where we were a few years ago," says Weatherford. "Are we where we need to be? No. But neither was PCI DSS when it first came out. Today, PCI DSS is a fairly good standard."

Weatherford has a number of areas where he'd like to see improvement. For instance, he would like the CIP standards to move more rapidly and possibly be augmented with

Powering Up Security

Utility company implements network encryptors to protect SCADA data and meet NERC requirements.

WITH A HUGE POWER PLANT built back in the 1 940s that covers a lot of square foot age, the North American Energy Alliance faced a compliance challenge. North American Electric Reliability (NERC) standards require that wiring bet ween physical securit y perimeters be enclosed in conduit, or the dat a must be encrypted. For the NAEA, that would have meant a lot of conduit, so it opted to encrypt, says Dominick Birolin, network engineer at NAEA.

The company, whic h is based in Iselin, N.J., and owns a portfolio of 1,755 megawatts of electricity producing power st ations in the Nor theast, looked at a variety of encr yption options, including point-to-point IPSec tunnels. But it determined that I PSec tunnels would result in latency problems, Birolin says.

"With CipherOptics, the latency was in microseconds as opposed to milliseconds. That was a big advantage, especially for SCADA systems."
–DOMINICK BIROLIN, network engineer, NAEA

NAEA ultimately c hose network encryptors from CipherOptics (now Cer tes Networks) for securing its SCADA information. CipherEngine Enforcement P oints from CipherOptics are F IPS 140-2 Level 2 validated encryption appliances.

"With CipherOptics, the latency was in microseconds as opposed to milliseconds. That was a big advantage, especially for SCADA systems," Birolin says.

The technology helps NAEA meet its compliance obligations, but data encryption is an overall good practice, he says.

–MARCIA SAVAGE

more agile ways for covered organisations to manage their risk. "It takes years for these standards to be agreed upon. That's way too long for cybersecurity," he says. Additionally, Weatherford says that a more dynamic risk management framework that can be used in conjunction with the CIP standards would help facilities more intelligently manage risk. "Just as all systems are not equally critical, the risk postures of different plants are not the same and can't be managed the same way," he says. "We've just begun work on developing a more agile way for organisations to leverage the CIP standards."

Assante also agrees that critical infrastructure regulations should be risk based and more agile to help better prepare critical infrastructures and the security teams that protect them. "Legislation should include the need for more sharply defined federal authority to address specific and imminent cyber security threats to critical infrastructures in the form of emergency measures," Assante said in a hearing before the Senate committee on homeland security and government affairs in November.

IMPROVING SECURITY OPERATIONS

When it comes to critical infrastructure protection, information sharing and collaboration has been called upon for years. Last year was the first year the industry has seen real information sharing begin to coalesce. In November, the Department of Homeland Security (DHS) launched a cyber security information sharing center designed to more efficiently share information about cyber threats to the critical infrastructure. Dubbed the Multi-State Information Sharing and Analysis Center (MS-ISAC) Cyber Security Operations Center, it's a 24-hour live watchdog that will, hopefully, provide state and local government officials the same details as those in the federal government.

According to DHS, The National Cybersecurity and Communications Integration Center (NCCIC) will head information sharing to the MS-ISAC Operations Center. States are expected to use the MS-ISAC Operations Center to cooperate to enhance IT security defense and response. The move is just one in a recent flurry of moves by the DHS to help bolster information sharing and incident response.

DHS also announced that the Information Technology Information Sharing and Analysis Center (IT-ISAC) will embed a full-time analyst and liaison to DHS at the NCCIC. The IT-ISAC consists of information technology representatives from the private sector and facilitates cooperation among members to identify sector-specific vulnerabilities and risk-mitigation strategies.

Also, this past fall, to test the nation's ability to withstand an advanced cyberattack, DHS and a number of international security and intelligence agencies engaged in a cyberwar game involving 1,500 security events designed to see how well federal agencies and more than 60 private-sector companies in critical infrastructure responded to a cyberattack. Cyber Storm III was used to test the newly developed National Cyber Incident Response Plan (NCIRP), which is the government's current cybersecurity incident response playbook. A report detailing the results of the exercise is expected soon.

"Government and industry aren't standing still, but the question is, are they doing enough, quickly enough," says IT Harvest's Stiennon.

HELP WANTED

In the future, it may not be budget, technological, or regulatory hurdles that prove the most challenging when securing the critical infrastructure; it could be finding enough skilled security professionals. "It's not that there's a problem finding security superstars; there's a lack of people with basic security skills and knowledge," says Vincent Liu, managing partner at the application security firm Stach and Liu.

In its report, *A Human Capital Crisis in Cybersecurity*, the CSIS found that there are roughly 1,000 security professionals in the U.S. who have the specialised cybersecurity skills needed to protect the critical infrastructure. The report estimates the nation could need up to 30,000 similarly skilled people to get the job done. "There's no doubt that we need to invest more in the security workforce. We need better training, and regular reassessments of their skill level," Assante says.

> "It's not that there's a problem finding security superstars; there's a lack of people with basic security skills and knowledge."
>
> –VINCENT LIU, managing partner, Stach and Liu

NERC's Weatherford agrees: "There are not many qualified, technical, cybersecurity experts that have experience in the power industry." He says it's part of a troubling macro trend affecting the IT industry. "We've been talking about the retirement bubble for a couple years now. We studied the issue when I was CISO at the state of California, and we found so many technical staff eligible for retirement within next few years that it became obvious that if we didn't train and recruit enough people, we were really going to have a problem," he says.

Having the IT staff needed to keep operations running smooth is one thing, having enough professionals trained in the still obscure IT security profession is another—and experts warn we are running out of time. "These aren't always highly skilled attackers or sophisticated malware that manage to get through. I've seen traditional worms like Conficker on hardened controllers," says Assante. "My greatest fear is that we are running out of time to learn our lessons. Stuxnet, although difficult to hijack or modify by others, may very well serve as a blueprint for similar but new attacks on control system technology," he adds.

George V. Hulme is a business and technology journalist who often writes about security topics from his home in Minneapolis, Minnesota. Send comments on this article to feedback@infosecuritymag.com.

The Client Side

ATTACKS ON APPLICATIONS LIKE ADOBE READER AND JAVA REQUIRE EFFECTIVE AND TIMELY PATCHING OF USER SYSTEMS.

BY MICHAEL COBB

THE PERVASIVENESS OF Microsoft Windows has made it a favourite target for hackers for years, but client-side applications like Adobe Reader and Flash Player are even more ubiquitous – a fact that hasn't escaped criminals. Dangerous vulnerabilities turn up in Adobe products on a regular basis. But it's not just Adobe vulnerabilities that put systems at risk. Serious security flaws have been found in other common client-side applications, such as Java, Apple QuickTime, Mozilla browser extensions, and Opera widgets.

Microsoft and many large vendors now release security updates and patches to a known timetable, and Microsoft products like Office can be automatically patched using the Windows Automatic Update. However, patches for other common applications such as Adobe Reader, Firefox, and Java can't. Relying on end users to manually install these patches distributes the patching workload but in no way is this ideal, as users can't be relied upon to get all the patches installed on a timely basis.

The timely patching of software vulnerabilities is critical to maintaining the operational availability and integrity of enterprise IT systems. Patching proactively prevents the exploitation of vulnerabilities, but the failure to keep application software patched

is one of the most common reasons why hackers are successful. Most major attacks in the past few years have targeted known vulnerabilities for which patches already existed. Although many organisations are competent at keeping their critical servers patched, the same level of attention isn't given to their users' desktops and laptops, even though statistically this is where most vulnerabilities occur.

According to vulnerability research company Secunia, the average computer needs about 76 patches per year from 22 different software companies. The logistics involved in keeping this number of applications patched is one of the reasons many applications remain unpatched. Read on for insight into how enterprises can manage the security of client-side applications and integrate fixes into existing vulnerability management programmes.

STANDARD BUILD

The single most effective method of improving patch management of client-side applications is to implement a standard build for desktops and laptops. A standard build will satisfy the vast majority of an enterprise's workforce and will help improve overall security. It reduces day-to-day maintenance and support costs, the number of different vendor alerts to follow and patches to test and deploy, and reduces the cost and time and overall burden of patch management. If every PC is configured differently, it becomes impossible to test patches on every permutation, leading to roll out problems and increased downtime.

Some employees will need non-standard applications and configurations, but this should be the exception not the rule. An application whitelist and controls to prevent users loading their own software will help control the number of applications you have to manage. To ensure non-standard machines are correctly maintained and patched, an up-to-date register of hardware and software should be established, recording installed applications, version information and all patches installed. If this register doesn't exist, Nmap is a free tool that can quickly gather this information. Each machine should be grouped by function, configuration and network location, and assigned a priority level. This helps to quickly identify which systems are most at risk to a particular vulnerability.

Even with standardisation, most businesses will still need to support a variety of applications from multiple vendors.

AUTOMATED TOOLS

To avoid the risky situation of unpatched machines on the network, most enterprises need to use an automated tool that pushes patches for different applications from different vendors from a central point. One such tool is Secunia's Corporate Software Inspector (CSI). Its Network Appliance Mode enables you to set up a CSI Agent as a remote-controlled dedicated scan engine, capable of automatically scanning complete network segments at scheduled intervals. It can identify about 13,000 applications from

2,300 companies on any network-connected machine, providing a complete software asset register, listing all the programmes and plug-ins installed on each machine and whether they're patched and up to date. The enterprise version allows you to automatically repackage a large number of patches from different vendors for direct deployment using groups and configurations from Microsoft's Windows Server Update Services (WSUS) or System Center Configuration Manager (SCCM).

Application patch status is checked by comparing installed programmes against Secunia's Vulnerability Intelligence database. The breadth and depth of this database means it can produce very accurate and detailed status reports, including criticality ratings for each insecure programme, along with detailed information about why it's insecure. It shows the full installation path, version details, and direct links to patches and Secunia Advisories, which provide additional details and metrics about the vulnerability as well as other useful information for alternative mitigation strategies.

Reports can also be used to verify that patches have been properly applied and old insecure versions have been removed, and to track the installation of non-approved applications, which is great for audit and compliance reports. It even lists end-of-life programmes. Software which has reached end-of-life should not be used, due to a lack of vulnerability information and the end of the vendor's commitment to providing security updates.

Other automated tools include Desktop Central, which supports managing both Microsoft and non-Microsoft patches, as well as pushing standardised application configurations to Windows machines on the network. It automatically identifies the new and latest updates, identifies the systems that need them and installs them. ManageSoft Security Patch Management provides a similar service, distributing and installing patches to Windows, Linux, UNIX, and Mac machines. It's important to note that any central patch management server needs hardening and protecting against malicious attack to prevent it being used as a tool to distribute malicious code.

When considering an automated system, you need to ensure that it can patch and update the software applications in use within your organisation.

When considering an automated system, you need to ensure that it can patch and update the software applications in use within your organisation. How it handles rollbacks of troublesome patches and tracks implemented patches for audit purposes are also important features to provide assurance that vulnerabilities have been identified and appropriate patches have been installed. Enterprise patch management tools are less efficient when unique deployments have to be managed, which is another reason why standardisation is good idea.

PATCH PRIORITISATION

Knowing which patches to install and when is another key element of good patch man-

agement. When a patch is released, attackers immediately try to reverse engineer it to identify the vulnerability and develop exploit code. This means the risk of attack increases immediately after the release of a patch, due to the time lag in obtaining, testing, and deploying it. Vulnerability criticality ratings are an important aid to help you prioritise your patch process, and accepted practice is to concentrate efforts on patches rated as critical and leave the others until a more convenient time. However, according to CERT, hackers are now starting to focus on vulnerabilities with lower ratings because they know it's likely that the relevant patches won't necessarily be installed so quickly.

This complicates the process of patch prioritisation and is why a risk-based approach is so important. All patches applicable to your software need to be recorded, but the first check is to see if it is relevant to your environment: Does it correct a vulnerability or problem in an application as it is being used within your organisation? For example, if your organisation disables browser scripting languages, then applying patches that fix scripting language vulnerabilities is not a priority. Other security controls may also automatically mitigate certain threats, again reducing the urgency to apply certain patches. If the vulnerability does put the organisation at risk, prioritise the patch by evaluating the impact it would have if exploited; for example, unauthorised system access, information confidentiality, arbitrary code execution, or denial of service.

If the overall degree of risk is not acceptable, then you must either apply the patch or pursue non-patch remediation; assume that exploit code is available for any vulnerability for which there is a patch. The next step is to determine whether the fix will affect the functionality of other software applications or services through research and testing. Testing should be performed on a selection of systems that accurately represent the configuration of the systems in deployment, since so many possible system configurations exist that a vendor can't possibly test against all of them. Check that all related software still operates.

A virtual test lab is essential for the efficient testing of patches on different platforms and configurations.

A virtual test lab is essential for the efficient testing of patches on different platforms and configurations. It greatly reduces your investment in hardware, space, and general overhead. It also means local administrators don't have to duplicate patch testing on their particular systems as they can all be replicated in the test lab.

VIRTUAL PATCHING

If applying a patch will impact business processes, you will need to agree to an appropriate time for patch installation and necessary downtime with system owners. When patch deployment has to be delayed, it may be possible to for some other compensating controls to be put in place. Known as virtual patching, changes such as a new firewall rule can eliminate the vulnerability by controlling inputs or outputs from the affected application; even the temporary removal of the application may be a sensible temporary option.

However, certain client-side applications and plug-ins, such as Adobe Reader, are going to be difficult to do without. In such instances, look for other ways of thwarting any potential exploits. For example, most users will not be inconvenienced if executable code embedded in a PDF document is disabled. Disabling JavaScript within Adobe will help prevent some of the more common exploits and you can still read a PDF document without JavaScript enabled. Many attacks can be successfully frustrated by ensuring that your users aren't logged on to their system with unnecessary elevated privileges; the majority will not need to have administrator rights on their desktop. This makes it a lot harder for an attacker to take complete control or cause widespread damage. Local administrators need to be informed of all vulnerability and remediation decisions.

PATCH DEPLOYMENT

Change management procedures should always be used when deploying patches, as systematic and documented processes are far more likely to result in a successful install. Even emergency patches need to go through this change-control process. Budgeted and approved resources, such as off-hours testing and overtime, need to be in place to make sure that they can be handled with the necessary priority. Manual methods may need to be used for operating systems and applications not supported by automated patching tools, such as experimental systems or those not part of Active Directory or a domain.

Java Exploits on the Rise

Cisco researchers say criminals now prefer Java over PDF.

Criminals last year began targeting Java more heavily than PDF to launch exploits, according to researchers at Cisco Systems.

According to the Cisco 2010 Annual Security Report, Java exploits made up 1.5 percent of Web malware blocked by Cisco ScanSafe in January 2010. By November, that number jumped to 7 percent. In comparison, PDF exploits dropped from slightly more than 6 percent to just 2 percent in the same time frame.

Cisco researchers surmise that the shift has to do with a number of factors, including increased availability of public Java exploit code and decreased availability of public Adobe Reader and Adobe Acrobat exploits. Some users also have shifted to other PDF readers or disable JavaScript in Reader.

The Blackhole, Crimepack and Eleonore exploit software packages make heavy use of Java, according to Cisco, which notes that Adobe Reader and Acrobat remain strong threat vectors online.

McAfee Labs, however, said malware developers heavily exploited weaknesses in Adobe products–Flash and particularly PDF technologies–throughout 2010. Malicious PDFs targeting Acrobat topped the number of unique samples collected by McAfee Labs, "making them the favourite target of client-side exploitation," the company said in its Q4 2010 Threat Report. The company expects the trend to continue this year as more mobile devices and non-Microsoft operating systems support Adobe technologies.› –MARCIA SAVAGE

For such computers, there should be written and implemented procedures for the manual patching process.

Even with standardised configurations and after thorough testing, it's still best practice to roll out patches to a small user group first before deploying them enterprise-wide. This allows user feedback and keeps disruption to a minimum if the patch does cause a problem for some unforeseen reason. Patches should certainly be deployed to standardised systems first before updating nonstandard and legacy machines.

Post-roll out tasks include verifying the patch installed properly by reviewing patch logs, checking that the vulnerability has been mitigated using a vulnerability scanner, updating configuration documentation, and documenting the decisions behind installing or rejecting specific patches.

Even with automated technologies in place, system administrators still need to subscribe and follow vendor alerts, vulnerability announcements, patch and non-patch remediations, and emerging threats. Relevant Internet forums, such as those offered by CERT, are also a great source of warnings of patch installation problems and problem solving advice. As with any security function, organisations need to measure the effectiveness of their patch and vulnerability management efforts, basically how quickly they can identify, classify, and respond to a new vulnerability and mitigate the potential impact within the organisation. This helps highlight any shortcomings in procedures or tools.

DIPLOMACY REQUIRED

Keeping enterprise users' machines secure is a tough task, given the relentless attacks on client-side applications like Adobe Reader and Java. Implementing effective patch management for user systems requires both technical and diplomatic skills. Getting business managers to accept that it is a regular business activity and not an optional one requires senior management support. Done well, it reduces the time and money spent responding to security breaches and helps protect the enterprise from legal and regulatory fines. Patching is much more cost-effective than responding to breaches; it's not possible to save money by neglecting patches.

Any opportunity to highlight the role patching plays in protecting the bottom line should not be missed, as manual patching of computers is getting harder to do effectively. Even moderate-sized organisations need a budget for a vulnerability scanner and an automated patching tool to make the process as effective and painless as possible for everyone.›

Michael Cobb, CISSP-ISSAP, CLAS, is a renowned security author with more than 15 years of experience in the IT industry. He is the founder and managing director of Cobweb Applications, a consultancy that provides data security services delivering ISO 27001 solutions. He co-authored the book IIS Security *and has written numerous technical articles for leading IT publications. Send comments on this article to feedback@infosecuritymag.com.*

Security breaches are going to happen. Don't get caught flat footed.

PREPARE FOR THE Inevitable

BY RAVILA HELEN WHITE

MOST IT LEADERS now know they must align with the business in order to be successful. However, one area where organisations continue to slip up is incident response planning. Enterprises spend copious amounts of time developing security policies and processes in order to secure systems and prevent breaches and data loss. Yet when a security breach occurs, they typically don't have a process in place to manage a coordinated response, within IT and external to IT.

There are a variety of reasons organisations may not have a coordinated incident response plan. Perhaps the organisation has invested in IT security, which is about technology, rather than information security, which focuses on strategy and business process. Part of that business component is incident handling. While incident handling is tactical in nature, it is driven out of programme strategy and is a process to manage tactical responses.

INCIDENT HANDLING DEFINED

Information security incident handling is an action plan for dealing with: intrusions (internal/ external), cybercrime (copyright violations, hate crimes, child pornography etc), disclosure of sensitive information or denial-of-service attacks.

For those of you who are familiar with the Information Technology Infrastructure Library (ITIL), you may wonder what the difference is between ITIL's incident management and information security's incident handling. A fine distinction exists in the fact that ITIL does not prepare an organisation to deal with events that may result in litigation. Additionally, where the root cause of an event in IT service management may be shared with customers, events which require infosecurity incident handling are typically confidential and considered "need-to-know." The final distinction lies in the difference between an event vs. an incident. ITIL defines any event that causes business disruption to customers or end users as an incident. In information security, events that require incident handling are related to security.

If your organisation has implemented ITIL, work to integrate the concepts of information security incident handling within your incident management process.

If your organisation has implemented ITIL, work to integrate the concepts of information security incident handling within your incident management process. Beyond promoting a common response for all events which disrupt services, there is the opportunity to embed security events as a normal part of business operations. In other words, it can act as a diffuser for you and your staff in that you are not the lone purveyors of seemingly bad news to the business. It is accepted that incidents of a security nature will occur and the appropriate rigour is in place for management.

PREPLANNING CONSIDERATIONS

Security incidents are unexpected regular events—the computing world's oxymoron. Any organisation with a connection to the Internet or that uses computers can expect to experience unexpected security events on a regular basis. Why? There are always vulnerabilities found and mistakes made; the regularity occurs with each release of software and each action taken by a technology user.

Due to the unexpected and stressful nature of security-related events, be prepared to devote your time and attention to the management of the incident. Detailed forms must be completed and descriptive notes taken. Likely, you will identify different types of security incidents resulting in specific procedures for each type of incident. However, it's unlikely your employer has the capacity to employ individuals whose primary responsibility is incident handling. Competing responsibilities reduce incident handling at its best to an ad hoc maturity level. Even with training and the right forms and procedures to guide you, it can be challenging to capture information correctly or follow instructions. Cooperation beyond the doors of IT is essential.

TEAMWORK REQUIRED

Incident handling is not an IT process but a business process that must be supported by the legal, human resources, communications and physical security teams of your organisation. Relationships must be built with these teams and expectations set in order to avoid conflict. Information security may drive the leadership of incident handling and provide the necessary training, however, a governance board of sorts should be assembled to oversee the process. Legal and HR must be involved to validate the legal soundness of your programme to ensure non-reputation of evidentiary data, which is a costly process.

Best-of-class technical environments are required to establish non-repudiation of evidentiary data. Dedicated hardware and specialised software is required along with training on the use of the software. Combined with the possibility of infrequent use, your business partners—the legal, HR and other teams—may challenge cost effectiveness. Be prepared to provide transparency around the cost of people, process, and technology. For organisations with regulatory obligations, the long-term investment should be part of the ROI strategy for selling incident handling. If your organisation does not have regulatory obligations, brand protection and reputation are legitimate considerations.

Discretion is an important element of information security incident handling. In ITIL's incident management process, outages and their root causes are shared with customers and business partners openly. In contrast, information security incident handling requires the discretion of all involved parties. Casual bandying of security incidents among employees can reduce the trust of internal business customers. More importantly, should the information find its way to customers or partners external to the organisation, damage to brand, reputation and trust will occur. Remember the principle of need-to-know (N2K) when handling incidents. Never talk to the press in response to a security incident unless directed by your legal team and senior leadership. Also, you can mitigate organisational Chatty Cathys by providing ongoing education and training.

Review all policies related to appropriate use and technology. While you may not directly write policy, you should familiarise yourself with your organisation's policies. Suggest additional policies supporting your incident handling plan. For example, work with the IT team to implement standards that will support the process. Some of the most seemingly granular discrepancies, such as overlooking clock synchronisation or log retention policies, can undermine the information you've gathered.

BUILDING OUT YOUR PLAN

Different types of incidents require different types of handling. Determining the response plan prior to an incident will streamline handling. Identify what types of incidents you may have to handle:

- Malware breach and containment
- Information disclosure
- Employee investigations

- DDoS attacks
- Hostile take-over

This may also be an opportunity to scope communications; knowing who needs to know in advance will help in avoiding unnecessary disclosure. For example, a DDoS attack does not require Need-to-Know (N2K): Most likely, sharing the cause of a network interruption with everyone will not damage brand or reputation.

Determining response plans prior to an incident will also help you pick the appropriate tools for recovering information. Identify what types of technology you may have to handle through technology scoping:

- Client PC technology
- PDA technology
- Cell phones
- Server technology
- Infrastructure technology
- Routers
- Switches
- Firewalls

Develop forms that will help you capture the information that is required for collection during an incident; SANS has a number of sample incident handling forms. Identify what types of documentation you will need to handle an incident through documentation scoping:

- Contact log—names of each point of contact during the incident;
- Evidence log—data points of information collected during the incident;
- Chain-of-custody log—audit trail of collected evidence when it changes hands;
- Communication log—information about incident and contact during initial incident notification;
- Sanitation record—information required for sanitised media;
- Recovery record—steps taken to recover from incident;
- Eradication log—steps taken to remove malware or hostile user;
- Identification record— type of incident and who discovered it.

PREPARE A TOOLKIT

Incidents can occur any time. You need a toolkit that provides access to all documentation required to capture incident information from beginning to end. When network compromises occur, you may not have the luxury of retrieving electronic documentation from the network. Having printed documentation ensures the information you capture is as accurate as possible. You must have the same documentation at home. Incidents are not considerate; they may happen at 3 a.m.

When possible, request dedicated technical resources, such as a spare drive for imaging and a spare workstation for gathering logs and performing other forsensics tasks for

incident handling. It is important to establish non-repudiation of the information you've gathered. Even if you cannot justify a dedicated server for storing recovered information, request storage that has limited access. Require periodic audits of the storage area controlled by keycard access to establish enforcement of access.

When handling incidents that require physical evidence recovery, store the hardware in a location that is secure, with limited access. You must also consider what collection tools you will use, such as log file analysers, disk imaging, and forensics software. Select commercial tools for information capture. Open source tools are cool, but organisations should purchase commercial tools to establish non-repudiation. If you do choose to use open source tools, clearly document them as part of your toolkit.

Costly Mistakes

Do not allow mistakes to derail your incident handling programme. Below are some of the most common and costly errors that undermine incident handling.

Disorganisation: Incident handling is useless if you do not have a plan or the appropriate forms for recording incident information. Waiting to develop a plan once an incident has occurred will result in disaster.

Rushing incident resolution: When an incident has occurred, it's important to dedicate adequate time to understand how the incident occurred in the first place. If the investigation is rushed, it may result in missing critical information or reintroducing a compromised system into your infrastructure.

Lone Ranger syndrome: Relying on your skills and expertise without engaging others. Depending on the maturity of your organisation, you may have to champion incident handling, but it's better to at least have the framework for a team and share that with proposed team members than to mishandle an incident and be left holding the bag.

Discounting Johnnie Cochran: If you assume that you will end up in court, then you should also assume that the court will want to understand how you collected your information. Litigation is all about proving or disproving a person's information. When you cannot provide documentation that would be expected of our industry, then all your handling may have been useless, along with your legal counsel and public relations.

Violation of need-to-know: Anyone who knows about the incident may have to testify in court. Stories vary in times of stress or through misinformation. Only those directly required to have knowledge of an incident should be briefed. Even then, tell them only what they need to know. Let your legal team determine whom outside of IT should be apprised.

Tunnel vision: Incident handling is more than just a detailed task; it's a business process. Take a strategic view when approaching incident handling.

–RAVILA HELEN WHITE

NOTE TAKING BEST PRACTICES

Take good notes, but keep in mind that lengthy notes containing unnecessary information are not helpful and will only muddy the incident, should it result in litigation. Notes must be informative, concise, and contain the facts of what you are handling. For instance, it is not necessary to mention that you are dealing with a suspected embezzler/child pornographer/ information thief, etc.; this is where your forms will assist. Complete generic fields prior to handling an incident. Record only those facts related directly to your evidence recovery:

- Who — contacted you; performed information recovery
- What — was recovered (e.g. log files)
- When — date and time of recovery
- Where — location of recovered evidence
- How — tools and method for evidence recovery

POINTS TO KEEP IN MIND

Any incident involving the recovery of information or technology associated with employee misconduct should be reported to your resident legal counsel. They will make the call regarding the appropriate actions to take. You should also notify legal should a third party who's been entrusted with your data experience a breach resulting in exposure.

Remember, incident handling is a business process that requires a plan. You will need a thorough understanding of your organisation to propose and implement a systemic plan. Once a plan is in place, update the process regularly. Just as disaster recovery plans and backups should be tested, so too should incident handling procedures. This will

ensure that the kinks are worked out prior to an incident.

Understand your responsibility. Incident handlers get into trouble when they go beyond the bounds of what is appropriate for their role. Only ask questions related to capturing relevant information. Beware of acting as a proxy to HR and legal when it comes to dealing with people. Do not go beyond the role of an incident handler. It's more trouble than it's worth.›

Ravila Helen White is the director of enterprise security and architecture at a company in the Pacific Northwest. Prior to that, she was the head of information security at The Bill & Melinda Gates Foundation and drugstore.com. Send comments on this article to feedback@infosecuritymag.com.

INFORMATION SECURITY EUROPE is published quarterly by TechTarget Member Services, Marble Arch Tower, 55 Bryanston Street, London W1H 7AA; Toll-Free 888-274-4111; Phone 617-431-9200; Fax 617-431-9201.

IT in Europe

INFORMATION SECURITY EDITION



COMING IN FALL 2011

What the Cloud Can Do For You: Choosing the Best Cloud Implementation For Your Business

The many possible permutations of the cloud—public, private and hybrid, to name the most common—each bring their own security concerns. Chossing one, and taking into account EU compliance mandates in the process, can be a difficult task.

Application Whitelisting

A technology operating in the kernel that detects suspicious changes in an IT-controlled software configuration should be easier to scale than a technology that looks at all files to identify and clean attacks. As such, pplication whitelisting makes too much pragmatic sense not to have appeal as an antimalware mechanism.

Social Engineering Awareness

Defending against today's social engineering attacks is difficult, but not impossible. It requires focusing on the human element of the equation with better security awareness training that gets employees to think twice about clicking on certain emails.

Don't miss our quarterly columns and commentary.

See ad page 2

- **Overview on the Importance of aWeb Application Firewall**
- **Securing Databases - Demonstration of Automated Monitoring, Auditing and Protection**
- **Monitor, Audit and Control Access to Sensitive File Data**

About Imperva:
Imperva is the global leader in data security. Our customers include leading enterprises, government organizations, and managed service providers who rely on Imperva to prevent sensitive data theft by hackers and insiders. The award-winning Imperva SecureSphere is the only solution that delivers full activity monitoring for databases, Web applications and file systems. To learn more about Imperva solutions visit http://www.imperva.com.