INFORMATION SECURITY®

EUROPE

SPRING 2011

Handle with Care

Calculating and managing risk is tricky business

also

5 WAYS TO INFLUENCE VENDOR MANAGEMENT

SECURITY AND DISASTER RECOVERY

TechTarget®

http://searchsecurity.techtarget.co.uk/

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*

IMPERVA

White Paper

Implementing Sarbanes-Oxley Audit Requirements

The Sarbanes-Oxley Act (SOX) of 2002 sets new requirements for the integrity of the source data related to financial transactions and reporting. In particular, auditors are looking at regulated data residing in databases connected to enterprise applications such as SAP, Oracle E-Business Suite, PeopleSoft, and other Web Applications.

To prove the integrity of data, companies must extend audit processes to the financial information stored within corporate databases. To verify regulatory compliance, auditors look at multiple aspects of a database environment including: user management, authentication, separation of duties, access control, and audit trail.

Auditors and information technology (IT) professionals must work together to prove that data usage in Oracle E-Business Suite, SAP, PeopleSoft and other package or custom applications meets SOX control requirements. Also, database administrator (DBA) and developer activity that takes place outside the structured business process of these applications must be monitored against controls.

In the following White Paper, we present the range of functions that need to take place to achieve and demonstrate compliance with SOX.

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®
Protecting the Data That Drives Business

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

contents

SPRING 2011
VOLUME 1 NUMBER 1

FEATURES

DEPARTMENTS

ALSO

Security Trends 2011: Making Sense of Predictions

While vendors have never been known to underestimate security threats, the job of the information security pro is, nevertheless, getting harder. BY RON CONDON

MANY IN THE security realm, vendors included, enjoy making predictions at year's end, and this time around, when it comes to the new year's security trends, 2011 is no exception. December and January had all the security vendors once again reaching for their crystal balls and making predictions.

Most of the forecasts make for uncomfortable reading, of course; no security company wants to admit that things are getting better, since there would be no need to buy any more of their products. They also tend to focus on the threats for which they believe they have a cure.

However, even if we strip out the predictions, hyperbole and the marketing, the raw data suggests that the job of information security is getting harder for a number of reasons.

On the one hand, threats are undoubtedly growing and changing. According to vendor and research firm Panda Security, 34% of all existing viruses were created during 2010. It adds that banking Trojans, such as Zeus, accounted for 56% of all new malware samples detected, and another 11.6% were fake antivirus software, a malware category that only appeared four years ago.

Botnets are also on the rise, according to ESET, another security firm, which detected 5,500 active botnets in November, compared to 4,000 the previous year. It forecasts that botnets could hit the 7,000 mark in 2011, partly because the criminals are using more and smaller botnets, which have a better chance of flying under the radar.

The reason for the growth is that cybercrime is a profitable business, and the chances of getting caught are slim.

The reason for the growth is that cybercrime is a profitable business, and the chances of getting caught are slim. Well-funded criminal gangs can buy the skills they need to create even more sophisticated malware.

And, working under a cloak of secrecy and false trails, these cybercriminals can disguise their locations and usually escape the attentions of law enforcement. They work globally, whereas police forces are constrained to their own jurisdictions. Although international police collaboration has improved in recent years, it is still too fragmented and slow-moving to block the activities of nimble crooks who owe no allegiance to any country and can readily

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
FACE-OFF
RISK MANAGEMENT
GOVERNANCE
DISASTER RECOVERY
SPONSOR RESOURCES

decamp to a less punitive jurisdiction if necessary.

Although most cybercrime is still directed at consumers' credit cards and banking details, corporate confidential information—with far greater commercial value—is now increasingly targeted. Advanced persistent threats, which involve slow and careful groundwork by the criminal to find chinks in the corporate armor, take more time and effort, but they play for much higher rewards.

Advanced evasion techniques are also being used to get past the filters of intrusion prevention systems, again using clever techniques to disguise incoming malware.

At the same time, it is becoming harder for organisations to keep track of their data. In the old days of the mainframe, data stayed on disks in the computer room. Now, there are a dozen ways for information to leave the corporate fortress, from webmail attachments to USB sticks, careless comments on social networking sites and smartphones. All these—and many other holes in the corporate sieve—provide a means for information to leak out, either by accident or by design.

Stuxnet also deserves a mention. Some see it as the grim face of malware to come; others see it as a targeted piece of code whose sole purpose was to disrupt the Iranian nuclear industry, and therefore is of no real relevance to the rest of us. Whatever the truth, it reminded those working with SCADA systems that they, too, need to raise their game against attack.

So there we have it: lots of new threats and an array of new ways for companies to lose their information. But does it change the way we need to do security in 2011?

Not really. The same principles apply, and the best organisations protect themselves by focusing their efforts on doing the basics well. That means identifying their most precious assets, and ensuring those are protected above all else. It also implies good identity and access management, to make sure only authorised users get to access the information they need to do their job.

Advanced evasion techniques are also being used to get past the filters of intrusion prevention systems, again using clever techniques to disguise incoming malware.

The best organisations also develop a culture of security. This is especially important now, since most security firms agree that in 2011 social networking sites will be a major channel for malware and other scams aimed at luring the unwary to infected websites.

For instance, security vendor Sophos Ltd. surveyed more than 1,200 users in December 2010 and found that 40% of social networkers had been sent malware, such as worms via the social networking sites of which they were members, a 90% increase since the summer of 2009. Two-thirds (67%) said they had been spammed via social networking sites, more than double the proportion two years ago, and 43% acknowledged being on the receiving end of phishing attacks, more than double the 2009 level.

While technology can help defend them, well-trained users are probably one of your best defences.›

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

CALL FOR NOMINATIONS

It's Time to Recognise the Industry's Best Security Professionals

Information Security magazine and SearchSecurity.com announce that nominations are open for the seventh annual Security 7 Awards. Find the nomination form at: http://www.surveygizmo.com/s3/462797/Security-7

Prestigious Industry Accolades

The honour roll of past Security 7 Award winners is a prestigious list of distinguished security practitioners and dignitaries, including Dorothy Denning, Gene Spafford, Michael Assante and Christofer Hoff. Since 2005, we've recognised the most innovative and stalwart security practitioners in the industry. It's time to do it again.

Seven Industries, Seven Winners

The Security 7 Award honors innovative security practitioners in seven vertical markets. We recognise the achievements and contributions of practitioners in the financial services, telecommunications, manufacturing, retail, government/public sector/non-profit, education and healthcare/pharmaceutical industries.

How to Nominate Your Peers

Do you know someone worthy of recognition? Nominate them by filling out the form. A panel of editors and industry experts will review the nominees and select our winners.

–MARK WEATHERFORD

2008 Security 7 Government winner

Former CISO for the states of California and Colorado and current CSO at the North American Electric Reliability Corporation (NERC)

INFORMATION SECURITY®

For more information, please visit our website: www.searchsecurity.com

Recognise the Security Industry's Best Today!

Smartphone Risk

Many organisations that allow smartphones to access their networks are woefully under-aware of the risks.

BY MICHAEL COBB

S **SMARTPHONES ARE RARELY** given the same level of risk assessment and protection as laptops, even though they introduce similar threats to business networks.

An incident involving a lost or stolen smartphone can escalate into a serious security event, potentially involving unauthorised access to data, voicemails and the network, unauthorised calls and inappropriate use of the Internet. An additional risk is the threat of eavesdropping; researchers recently demonstrated how mobile calls and texts made on any GSM network can be eavesdropped upon using four cheap phones and open source software.

Smartphones need to be locked down—many insecure features are enabled by default—in much the same way as laptops, and laptop security policies can be used as a baseline for a corporate smartphone policy.

Businesses, however, must reassess each control from the viewpoint of an attacker in order to develop more effective rules and safeguards to limit the risks smartphones pose. For example, take passwords and idle timeout rules. An excessively long timeout setting could allow an attacker to access data or install spyware, while too short a period requires repeated re-entry of the password, making it easier for an observer to record it.

Strong alphanumeric passwords can be problematic on certain smartphones without a QWERTY keyboard, which highlights the need to assess a phone's security features to ensure it can adhere to your policies. Ease of integration of its email, contact and calendar applications with existing technologies such as Active Directory is also an important consideration.

Encryption is another area to focus on. Full device-level encryption can hamper performance and battery life, but it means all data is effectively unreadable, even if a device finds its way into the wrong hands. It's also less complex than file- or folder-level encryption with regard to data classifications and user interaction. In short, full encryption has become a must-have for any user with high-level access to ensure compliance with polices and regulations.

Depending on your use case, you may need to consider third-party encryption products that can protect the phone as well as its removable SD cards. This may be necessary in meeting certain data and regulatory requirements.

While security technologies like encryption can go a long way toward mitigating risk, good policy planning and enforcement can do even more. For instance, phones should never be allowed to store personal information about customers or intellectual property.

Access to the corporate network using a smartphone should not only be based on the user's role in the business, but also on his or her location and the connection used, such as from inside or outside the corporate network, or through a VPN. For example, a connection via an unsecured Wi-Fi network that is not going through the corporate VPN should be blocked.

VPN access should also be restricted to specific business tasks, as an 'access all areas' approach is not necessary and is too risky. Extending network access control (NAC) technology can provide the necessary checks to establish a phone's access rights based on its patch and antivirus status and application configurations.

Other policies, such as backups, need to be extended to smartphones, but care should be taken that this safety net doesn't reduce users' sense of duty just because their data is backed up somewhere else. Users need to appreciate that losing a phone is not just an inconvenience to them, but potentially a data breach. There has to be a strong focus on avoiding loss or theft: An average of 10,000 mobile phones are left in the back of London taxis every month, compared to 1,000 laptops. A few minutes of physical access to a phone is all that's needed to download and install off-the-shelf spyware.

Extending network access control (NAC) technology can provide the necessary checks to establish a phone's access rights based on its patch and antivirus status and application configurations.

To reduce theft or misuse, smartphone risk training for end users has to emphasise information asset ownership and physical security awareness. Employees who understand that they must take responsibility for an organisation's information assets dramatically improve the strength of its security. Stronger disciplinary measures—including suspension or even termination in the event of a serious breach of policy—may need to be introduced to focus people's attention on safeguarding their phones.

Smartphones need to be seen as an extension of the network with standard security maintenance. This involves patch management with administrators following relevant mailing lists to keep on top of firmware and OS updates. User groups and forums are also useful for tackling end-user issues and vulnerabilities. Servers devoted to smartphone applications need to be hardened, with careful attention paid to authentication and authorisation controls.

Enterprise-level smartphone security hasn't, in the past, been a focus of vendors, but this is changing. Centralised management and directory services that provide device monitoring and audit trails, and that push phone and policy settings are improving, and there's a growing range of products from vendors such as Symantec Corp., McAfee Inc. and Trend Micro Inc. that support enterprise-wide password management, application lock down, data port disablement and the ability to remote kill a lost device.

However, features such as locking down cameras or disabling SD card slots are still mainly works in progress, and many mobile applications are poorly written from a security standpoint. Antivirus and antispam applications aren't as mature as their desktop equivalents. Thus, it's essential that the risks from these shortcomings be assessed, as the only remedy is appropriate usage by each user.

Smartphones do open holes in standard network defenses, so risk management is essential to allow the benefits they bring, while avoiding breaches in security. The Stuxnet worm highlights how IT infrastructures need to adapt their security to meet new threats, so managing smartphone risk should be a top priority for IT departments everywhere.›

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.

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

FACE-OFF

RISK MANAGEMENT

GOVERNANCE

DISASTER RECOVERY

SPONSOR RESOURCES

ANALYSIS | CRITICAL INFRASTRUCTURE PROTECTION

Ranking the Global Cyberthreat

What's the real threat of global cyberwar, and how vulnerable are IT infrastructures? BY RON CONDON

A REPORT TO the 34-nation Organisation for Economic Co-operation and Development (OECD) has warned governments to keep cyberthreats in proportion and not to entrust the defence of critical national infrastructure to the military.

The report, "Reducing Systemic Cybersecurity Risk", co-authored by Professor Peter Sommer of the London School of Economics and Dr. Ian Brown, a senior research fellow at the Oxford Internet Institute, University of Oxford, concludes that a cyberwar fought solely in cyberspace is highly unlikely, but it does concede that a cyber element will feature in any armed conflict.

However, they insist that few single cyber-related events have the capacity to cause a global shock, and that most breaches of cybersecurity would be "both relatively localised and short-term in impact."

The authors argue that the term cyberwarfare is used too liberally to describe any cyberthreat, and that a lack of clear definitions could lead to governments allocating funds in a way that does not actually provide defences.

While acknowledging the importance of the Internet and associated systems to modern economies, and the known threat of state-sponsored espionage, it insists that, "Cyberespionage is not 'a few keystrokes away from cyberwar, the report is one technical method of spying. A true cyberwar is an event with the characteristics of conventional war but fought exclusively in cyberspace." The comment may be a veiled response to some of the controversial statements made by former White House special advisor to the president on cybersecurity, Richard Clarke, who has warned against state-sponsored cyberattacks in a series of books.

One of OECD's charges is that governments are paying too much attention to the potential damage a military or global cyberthreat could incur, and risk ignoring the far more likely effects of an accidental or systemic failure.

"A lot of people are using the term cyberwarfare far too loosely," Sommer said. "When

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
FACE-OFF
RISK MANAGEMENT
GOVERNANCE
DISASTER RECOVERY
SPONSOR RESOURCES

you press them what they mean and ask if the effects would be as devastating as [those of the war] in Afghanistan, or the Middle East, for example, they start to back down."

Sommer said it is a mistake to use the term cyberwar to describe espionage, hacktivist blockading or defacing of websites, as recently seen in reaction to the arrest of WikiLeaks founder Julian Assange. He said it was "not helpful to group trivially avoidable incidents like routine viruses and frauds with determined attempts to disrupt critical national infrastructure."

The report says that many cyber risks are real, but that it is important to test each one to understand all the elements that would have to be in place before a potential threat could cause real damage.

The report also acknowledges known attacks in recent years against Estonia, Georgia, Lithuania and South Korea, where government, banking and media websites came under fire, but makes the point that, although the attacks were "annoying" and "embarrassing," they did not involve violence or destruction.

Brown put much of the blame on security vendors for exaggerating the dangers in order to sell products. "People quote huge numbers of attacks per day on government systems to show how bad the problem is, but they are counting every last probe and phishing email," he said. "You have to be careful about crying 'wolf'. It will catch the eye of the public the first time you do it, but they will very quickly get bored, especially if they don't see it leading to any negative outcomes that affect them. There is already an undercurrent of scepticism and cynicism from commentators saying the threat is overblown."

"The military needs to do a lot to protect its own systems, but that doesn't put it in a good position to go out and solve this in the wider economy. The problem is much broader and goes across the private sector."

–DR. IAN BROWN, senior research fellow, Oxford Internet Institute, University of Oxford

The authors underline what they see as the hazard of giving the military all responsibility for handling such threats. "There's a danger of money and effort being wasted if [cyberwar is] treated purely as a military threat," Brown said. "The military needs to do a lot to protect its own systems, but that doesn't put it in a good position to go out and solve this in the wider economy. The problem is much broader and goes across the private sector."

He said that the private sector and parts of government, such as the UK Department for Business, are best equipped to deal with many of the threats, especially since much of the UK's critical national infrastructure is in private industry.

However, the report does emphasise the fragility of much of the technology that underpins modern life. For instance, it examines the growing complexity of modern software, pointing out that while Windows NT 3.1 in 1993 had 4.5 million lines of source code, its successor Windows NT 3.5 in 1994 had 7.5 million lines, and Windows XP, released in 2001, had 40 million. "If we assume only one bug or error per 1,000 lines, we arrive at the possibility of 40,000 bugs in Windows XP," it says.

The report also warns that some current trends—such as government agencies relying on the open Internet to deliver services, and the rise of cloud computing—open up systems to more damaging attacks unless proper defences are put in place.

"With appropriate industry standards and competition between providers, it should be possible for businesses to manage the day-to-day security risks associated with cloud computing," conclude the researchers in their report. "However, less attention so far has been paid to the impact of catastrophic events on cloud services. Without careful resilience planning, customers risk a loss of processing capacity and of essential data."

The report lists a range of threats, ranked by the damage they could do and the time it would take to contain them. The conclusion: Only a successful wide-scale attack on the Internet infrastructure would be enough to cause serious and lasting damage. To further underscore the view that governments need to pay attention to IT infrastructure risks that don't necessarily involve attackers or malicious activity, the report posits that a serious solar storm is one of the most dangerous threats, and could do widespread damage to the electrical grid.▸

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

FACE-OFF

SECURITY EXPERTS **BRUCE SCHNEIER & MARCUS RANUM** OFFER THEIR OPPOSING POINTS OF VIEW

Is a software monoculture dangerous to computer security?

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
FACE-OFF
RISK MANAGEMENT
GOVERNANCE
DISASTER RECOVERY
SPONSOR RESOURCES

POINT: **BRUCE SCHNEIER**

In 2003, a group of security experts—myself included—published a paper saying that 1) software monocultures are dangerous and 2) Microsoft, being the largest creator of monocultures out there, is the most dangerous. Marcus Ranum responded with an essay that basically said we were full of it. Now, eight years later, Marcus and I thought it would be interesting to revisit the debate.

The basic problem with a monoculture is that it's all vulnerable to the same attack. The Irish Potato Famine of 1845–9 is perhaps the most famous monoculture-related disaster. The Irish planted only one variety of potato, and the genetically identical potatoes succumbed to a rot caused by *Phytophthora infestans*. Compare that with the diversity of potatoes traditionally grown in South America, each one adapted to the particular soil and climate of its home, and you can see the security value in heterogeneity.

Similar risks exist in networked computer systems. If everyone is using the same operating system or the same applications software or the same networking protocol, and a security vulnerability is discovered in that OS or software or protocol, a single exploit can affect everyone. This is the problem of large-scale Internet worms: many have affected millions of computers on the Internet.

> **If our networking environment weren't homogeneous, a single worm couldn't do so much damage.**
>
> –Bruce Schneier

If our networking environment weren't homogeneous, a single worm couldn't do so much damage. We'd be more like South America's potato crop than Ireland's. Conclusion: monoculture is bad; embrace diversity or die along with everyone else.

This analysis makes sense as far as it goes, but suffers from three basic flaws. The first is the assumption that our IT monoculture is as simple as the potato's. When the particularly virulent Storm worm hit, it only affected from 1–10 million of its billion-plus possible victims. Why? Because some computers were running updated antivirus software, or were within locked-down networks, or whatever. Two computers might be running the same OS or applications software, but they'll be inside different networks with different firewalls and IDSs and router policies, they'll have different antivirus programmes and different patch levels and different configurations, and they'll be in different parts of the Internet connected to different servers running different services. As Marcus pointed out back in 2003, they'll be a little bit different themselves. That's one of the reasons large-scale Internet worms don't infect everyone—as well as the network's ability to quickly develop and deploy patches, new antivirus signatures, new IPS signatures, and so on.

The second flaw in the monoculture analysis is that it downplays the cost of diversity. Sure, it would be great if a corporate IT department ran half Windows and half Linux, or half Apache and half Microsoft IIS, but doing so would require more expertise and cost more money. It wouldn't cost twice the expertise and money—there is some overlap—but there are significant economies of scale that result from everyone using the same software and configuration. A single operating system locked down by experts is far more secure than two operating systems configured by sysadmins who aren't so expert. Sometimes, as Mark Twain said: "Put all your eggs in one basket, and then guard that basket!"

A single operating system locked down by experts is far more secure than two operating systems configured by sysadmins who aren't so expert.
–Bruce Schneier

The third flaw is that you can only get a limited amount of diversity by using two operating systems, or routers from three vendors. South American potato diversity comes from hundreds of different varieties. Genetic diversity comes from millions of different genomes. In monoculture terms, two is little better than one. Even worse, since a network's security is primarily the minimum of the security of its components, a diverse network is less secure because it is vulnerable to attacks against any of its heterogeneous components.

Some monoculture is necessary in computer networks. As long as we have to talk to each other, we're all going to have to use TCP/IP, HTML, PDF, and all sorts of other standards and protocols that guarantee interoperability. Yes, there will be different implementations of the same protocol—and this is a good thing—but that won't protect you completely. You can't be too different from everyone else on the Internet, because if you were, you couldn't be on the Internet.

Species basically have two options for propagating their genes: the lobster strategy and the avian strategy. Lobsters lay 5,000 to 40,000 eggs at a time, and essentially ignore them. Only a minuscule percentage of the hatchlings live to be four weeks old, but that's sufficient to ensure gene propagation; from every 50,000 eggs, an average of two lobsters is expected to survive to legal size. Conversely, birds produce only a few eggs at a time, then spend a lot of effort ensuring that most of the hatchlings survive. In ecology, this is known as r/K selection theory. In either case, each of those offspring varies slightly genetically, so if a new threat arises, some of them will be more likely to survive. But even so, extinctions happen regularly on our planet; neither strategy is foolproof.

Our IT infrastructure is a lot more like a bird than a lobster. Yes, monoculture is dangerous and diversity is important. But investing time and effort in ensuring our current infrastructure's survival is even more important.

Bruce Schneier is chief security technology officer of BT Global Services and the author of Schneier on Security. *For more information, visit his website at www.schneier.com.*

COUNTERPOINT: MARCUS RANUM

"YAWN! The death of the Net predicted"….

Eight years later, monoculture remains a poor and misleading comparison. Why do we need to analogise about computers as if they were biological systems? We ought to be perfectly capable of assessing them on their own terms. We have a rich vocabulary of security terminology, based on a set of commonly understood principles, so why do we feel it's important or useful to squint hard and say, "Computers are kind of sort of like biological organisms; therefore, they're likely to fail in similar ways"? Computers fail like computers, and organisms fail like organisms—any resemblances between the two are largely coincidental.

Let me illustrate how silly these analogies can get with a simple thought experiment. Suppose for a few minutes we're going to pretend a network plus a bunch of computers is an organism. We can construct one analogy that sounds pretty scary by saying, "Computers, of course, don't have an immune system." Or, we can construct another analogy by saying, "The system administration team plus the combined security researchers at all the antivirus/antimalware vendors plus configuration management software is the immune system." See what I mean? We're wasting time arguing about which analogy is better, which is pointless. It makes more sense to talk about computer security problems using the language of computer security, which is rich enough, even if you exclude the marketing buzzwords.

Computers fail like computers, and organisms fail like organisms—any resemblances between the two are largely coincidental.

–Marcus Ranum

In fact, the monoculture concept only seems to carry zing because the biological metaphors obscure the basic silliness of the concept. Talking about it in the language of computer security, what the monoculture fearmongers are saying is something (trying to be fair) like: "Too many computers share a common operating system, and therefore share its common flaws; consequently, at a certain point a shared vulnerability could be used to cause massive, cascading failures of critical infrastructure. Therefore, be very afraid."

However, in the real world we observe that:

- The first part of that scenario has already happened; in fact, it has happened about once a week for the last 15 years.
- The second part of that scenario hasn't happened, or even anything close to it.

Why not? Because every computer/network out there is managed differently, patched differently, has different addressing and routing schemes, different firewall rules, different configuration management practices, different diagnostic and analytic capabilities, and different system administrators. If you don't get blinded by the shiny analogy, you realise pretty quickly why the monumental collapse scenarios haven't happened since Robert Morris, Jr. took down a small but significant percentage of the nascent Internet for several hours, back in 1988.

There are large numbers of systems that are managed and configured in lock-step—for example, smartphones, certain point-of-sale terminals, and ATMs. Generally they tend to be special-purpose systems, "walled gardens," or consumer-oriented systems which need zero demand for system administration. In fact, many of those systems run Microsoft Windows—the very stuff that the monoculture paper warned us about. But there haven't been meltdowns, outside of the occasional entire application-specific load-out (such as one particular bank's ATM network, or a specific wireless provider's smart phone) toppling over, briefly. What we see is exactly what we'd expect to see if the monoculture idea were absolutely wrong: Whenever a new vulnerability is discovered, some systems topple, some are immune, some quickly react with workarounds, and home users wonder why their personal computers have suddenly gotten a bit slower.

> **Whenever a new vulnerability is discovered, some systems topple, some are immune, some quickly react with workarounds, and home users wonder why their personal computers have suddenly gotten a bit slower.**
>
> –Marcus Ranum

A more formal explanation why monoculture isn't a problem can be found in Charles Perrow's 1999 book "Normal Accidents," in which he analyses failures in terms of the complexity and interdependence of systems. In Perrow's worldview, a system can be said to be "tightly coupled" if the correct function of one component depends subtly on another, and another in turn. The greater the degree to which components are interdependent, the more likely they are to experience complex, unpredictable accidents—accidents that Perrow says are easily enough understood in hindsight but are nearly impossible to model predictively because the interdependencies are not discoverable in advance of the accident.

Now, consider modern networks, systems, and software in that light: some pieces are interdependent and others aren't. Yes, a lot of systems depend on components such as DNS, but the upper layers "understand" that it's a piece of the system that fails, and try to fail gracefully along with it. You won't, however, see one service provider building deliberate interdependencies with a competitor unless it's angling for a featured spot on

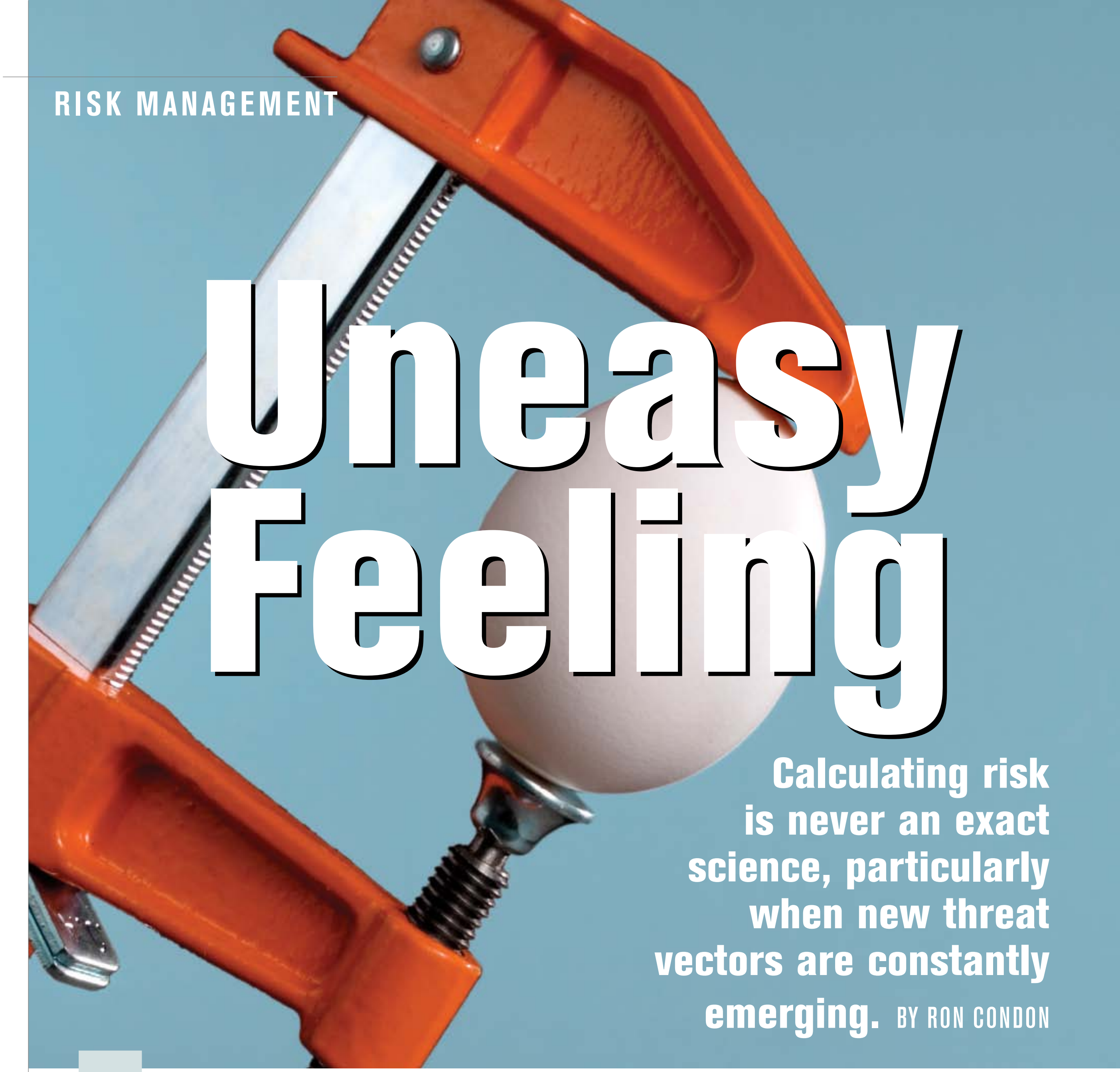
FAIL Blog. The systems and networks we depend on are exactly as wobbly and unreliable as they possibly can be, and yet still function; failure is a built-in fact of the environment, and that's why "belt and suspenders" remains the byword of geek chic.

The monoculture argument was, barely concealed, nothing more than an extended whine about Microsoft's market dominance—and I happen to know that the main authors were all Mac users. I suspect that security was less the real issue than the frustration Mac users felt a decade ago at being blown off by corporate IT. But look what's happened: the technology landscape has changed, and now there are two completely different operating system/application stacks—neither of which has yet toppled in a catastrophic failure.

That's partly because of market dynamics; it seems that when one vendor gains a sufficiently strong lock on a market it over-prices and under-innovates until a cheaper, cooler, and shinier alternative becomes attractive. The entire history of the computer industry is a swirling jumble in which one company dominates enough to become scary and create its competitors—the way IBM's lock on business computing in the 1970s triggered the departmental computing revolution of the 1980s, and "big IT" and system administration in the 1990s justifies the "cloud computing" backlash.

Monoculture won't happen because every vendor needs to differentiate its products in the marketplace if there is still room to innovate. The "all the eggs in one basket" scenario you're worrying about is a natural reaction to the vendor-inspired technology fragmentation of the 1980s; it's just the normal ebb and flow of the market. ▸

Marcus Ranum is the CSO of Tenable Network Security and is a well-known security technology innovator, teacher and speaker. For more information, visit his website at www.ranum.com.



Uneasy Feeling

Calculating risk is never an exact science, particularly when new threat vectors are constantly emerging. BY RON CONDON

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
FACE-OFF
RISK MANAGEMENT
GOVERNANCE
DISASTER RECOVERY
SPONSOR RESOURCES

THE BANKING CRISIS of 2008 did much to dent the reputation of risk management as a discipline.

With their teams of Ph.D. geniuses, the banks had created what looked like unbreakable predictive models to help them manage the risks implicit in allowing more and more people to take out mortgages, which a staggering number of customers were never able to repay.

When the whole banking system collapsed like a house of cards, the pseudo-scientific mathematical formulae that underpinned the businesses (and which, it emerged later, few people understood) were revealed to be more pseudo than scientific. Their complexity had provided a veneer of reassurance, but their failure came as a stark reminder that risk calculation is by no means synonymous with risk mitigation.

It is a lesson that information security professionals should heed: system controls, policies and procedures designed to cope with last year's problems can be easily rendered ineffective by this year's new and emerging threats.

For example, no sooner have organisations decided how to handle USB sticks than they have other questions to answer, such as how to deal with smartphones, iPads and social networking sites; users' requirements for technology often outstrip the security team's ability to protect their devices.

And 2011 will no doubt introduce even more must-have gadgets, plus new forms of malware presented by an ever more resourceful criminal underworld. Add to that the rise of Internet-based campaigns by special interest groups such as those that sprang to the defence of WikiLeaks founder Julian Assange, and the possibility of state-sponsored cyber aggression, and it would be a brave or foolish person who would claim to have it all under control.

Handling emerging threats

AT LLOYD'S OF LONDON

THE INFORMATION THREAT landscape is in constant flux. It is essential to find a way of coping with new dangers as and when they arise. Unless organisations have already done the basic work to establish a risk management process and infrastructure, each new threat can create panic and kneejerk reactions.

At Lloyd's of London, senior information risk and protection manager Marcus Alldrick has developed a process that brings emerging threats into the mainstream risk management process and allows them to be considered by the business in an organised fashion.

As a bellwether for the insurance industry, Lloyd's has been assessing risk for hundreds of years, so the concept is well understood by all in the company.

However, as with many security-related projects, it is a new piece of regulation–the Solvency II rules being introduced by the EU by the end of 2012 to regulate the solvency of insurance firms–that provided the trigger to formalise Lloyd's handling of emerging threats.

To respond to this regulation, Lloyd created the Emerging Technology Threats Forum, an internal group that meets regularly with representation from all parts of the business, including marketing, legal, compliance and IT.

Current subjects under review by the forum are smartphones, social networking, cloud computing and advanced persistent threats. "These subjects come up for discussion, and we decide if they constitute a threat or a risk," Alldrick says. "If we feel we need to deal with one, then we gather as much information as we can, and produce a white paper, which then forms part of a recommendation to the corporate management. It means that we are moving forward on the basis of informed risk. We don't take kneejerk decisions."

In the case of the iPad, for instance, there are no real metrics yet to show what kind of risk it might pose, and so Lloyd's is carrying out a small pilot trial to learn more. "We'll look at what controls are currently in place and where we could face a risk, and what we would do to mitigate the risk," Alldrick says. If we can't mitigate the risk, then we will constrain [the device's] use."›

–RON CONDON

Nevertheless, risk management is an essential part of information security, and organisations must do their best to protect their most valuable assets against whatever new business risks fate may throw at them. Assessing any kind of risk will always involve some level of guesswork; the skill is in reducing the margin of error to an acceptable level.

Back to basics

Risk is generally calculated by combining the likelihood of a threat and its potential effects. To take a simple example: It is a sure bet that there will be viruses on the Internet, and the effect of viruses on an organisation's systems, if left unchecked, would undoubtedly be disruptive, to say the least. Therefore, the risk is high, and the company must apply a mitigating control (such as antivirus software and firewalls) to manage the risk.

So far, so easy: In this example, the negative effects and ubiquity of viruses are well established, and antivirus software is not too expensive.

The picture becomes more complex when any of the factors are less certain, or if the cost of a mitigating control is too high. For instance, how important is proper function of an enterprise's payroll system? Obviously, it is vital to pay workers, but, in reality, the loss of the system for a few days (as long as none of them are pay day) would have little impact.

The security pros can probably estimate the reliability of a server, but they alone cannot determine the business effects, nor the cost of the mitigating control (the standby server). Those things are down to the business, and its appetite for risk.

How likely is it that the payroll server would go down (via a virus, or even a simple hardware or software failure)? This is a key question when determining how much to invest in its security and redundancy. Probably, with good maintenance, the payroll server is unlikely to break down, and with standard security practices, the payroll system is typically secured with relative ease, so the risk is probably not high enough to justify having a standby server. The payroll manager may not agree, but the business may decide it's a risk it can live with.

Which leads to the next question: Who decides when it comes to the impact and likelihood of risk? The security pros can probably estimate the reliability of a server, but they alone cannot determine the business effects, nor the cost of the mitigating control (the standby server). Those things are down to the business, and its appetite for risk.

Planning a risk assessment

Nick Frost, global account manager for the Information Security Forum, a membership organisation comprised of more than 300 major corporations, has spent the last 10 years researching risk management. He says the best companies have shifted their focus from

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
FACE-OFF
RISK MANAGEMENT
GOVERNANCE
DISASTER RECOVERY
SPONSOR RESOURCES

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
FACE-OFF
RISK MANAGEMENT
GOVERNANCE
DISASTER RECOVERY
SPONSOR RESOURCES

individual IT systems to business processes. The effect has been dramatic.

"The planning and scoping of risk assessments has improved beyond recognition from what I saw 10 years ago," he says. "It used to be done at a system level and in an ad hoc manner, and organisations targeted what the IT manager thought was the most important system, such as email or the public website. There was a disconnect between what the business thought was important for them, and what the IT function considered to be important."

The best companies, he says, now plan their risk assessments according to their most critical business processes. "Before they even start thinking about systems that need to go through a risk assessment, they identify the critical processes," he says.

If, as is usual these days, the organisation has mapped its business processes, the information risk manager has a perfect starting point for planning and scoping an assessment of the most critical processes. "The best CISOs look at processes, not just systems," he says. "They can then determine which are the systems that are fundamental in keeping that business process working."

The benefit of focusing first on the process level is that the assessment can incorporate a broader and more practical list of the types of security threats. These can include accidental threats, such as people entering the wrong data by mistake, for example, and the resultant assessment tends to be more complete, rather than focusing just on technical faults.

"Every business owner thinks his or her system is the most important, so if you have a structured way of assessing criticality, you force the owners to use a company-wide yardstick to measure what could go wrong if a system were down for a day, or if they had a breach of confidentiality."

–SIMON OXLEY,
cofounder and managing director, Citicus Ltd.

Classifying assets

Having identified critical processes, risk managers can then start classifying the information assets of the organisation, which can include applications and data as well as servers and networks.

The aim is to build an inventory of the assets and to understand their relative importance to the organisation, which needs to be done in a structured and objective way.

"Most organisations have a gut feeling about what is important, but when they take a structured and objective approach, organisations can be surprised by what is revealed," says Simon Oxley, one of the founders and the managing director of Citicus Ltd., which sells consultancy and software to support risk assessments. "Every business owner thinks his or her system is the most important, so if you have a structured way of assessing criticality, you force the owners to use a company-wide yardstick to measure what could go wrong if a system were down for a day, or if they had a breach of confidentiality."

Oxley favours a standard approach, which forces each business owner to rank the criticality of his or her assets by assessing the damage that could occur if the asset was compromised for an hour, a day or a week. How serious would the damage be in terms of profits, performance and reputation? That then allows the organisation to identify which are the most sensitive systems.

"It's not rocket science, but if you have a structured approach, it just helps you to channel your efforts and cash more effectively," Oxley says.

"Some organisations start by thinking they have a lot of critical information systems, but they find they only have a handful that are really critical to the organisation; the others are important to the people responsible for them, but they are not critical."

The exercise can also uncover some uncomfortable truths, he says, such as a critical business process running on an Excel spreadsheet that the user has developed alone, without an external code review. "When you begin the process, you may think the critical assets are the big business applications (such as finance or payroll), but it is often a surprise how big a role these spreadsheets play. Organisations discover they don't have a lot of control over them, and that they run the risk of data integrity problems," Oxley says.

> "It's not rocket science, but if you have a structured approach, it just helps you to channel your efforts and cash more effectively."
>
> –SIMON OXLEY, cofounder and managing director, Citicus Ltd.

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
FACE-OFF
RISK MANAGEMENT
GOVERNANCE
DISASTER RECOVERY
SPONSOR RESOURCES

The risk assessment process

Having identified the critical business processes, and the critical information assets that underpin them, then a more detailed assessment of risks can begin. This is probably the most demanding and arduous part of the process, because it requires all parts of the business to come together to assess the risks, with the meetings facilitated by an information security professional.

"We encourage people to do workshop-based risk assessments," Oxley says, "where you pull together the business person responsible for the assets, plus those with information about the risk: IT operations, IT development and internal auditors. You use a risk scorecard in the discussion, and the interplay of their different perspectives helps to get a realistic picture of the risk."

The workshops generally last for no longer than two hours to avoid attention fatigue, and they can bring to light some incongruent views, Oxley says. For instance, a business owner may report that the applications are running fine, whereas users may be aware of problems that have occurred.

In another instance, a business owner reported that his system had experienced recurring problems. In the workshop, IT operations explained that the system shared a server with another application that was causing all the trouble. Operations assumed there was no budget for a dedicated server, but once the business owner learned the truth, he provided the money to make it happen. “No one had asked him if he’d pay for a separate server before,” Oxley says. “There is a lack of communication within organisations, and this leads to people taking decisions based on their own perceptions without using a structured approach.”

Preparing for the worst

Like it or not, some threats cannot be managed. A sustained attack by a foreign power—such as Operation Aurora of a year ago, determined DDOS attacks and new malware such as Stuxnet—could all be impossible to prevent, either because they exploit unpatched vulnerabilities, or because of the sheer force they apply.

According to ISF’s Frost, many organisations now conduct what are essentially tabletop exercises in order to plan how they would react to the kind of eventuality where, for example, an unstoppable infection was spreading on the network, or a system had been put out of action by a DDoS attack, and the attackers were asking for a ransom.

> “By doing the cyber-response exercise, business managers can see what could go wrong with their side of the business.”
>
> –NICK FROST, global account manager, Information Security Forum

The response exercise takes the form of a meeting, attended by senior managers representing affected units, where a threat scenario is proposed. Their task is to decide what would be the best course of action.

A well-prepared exercise will keep introducing new uncertainties. For instance, after a server goes down and a standby machine begins running its application, this secondary server is then brought down as well. “By doing the cyber-response exercise, business managers can see what could go wrong with their side of the business,” Frost says. “So when a list of controls is presented after the exercise, he or she is in a much better position to decide if the controls are applicable, and to understand and acknowledge their security functions.”

Further reading

SANS Introduction to risk management

HM Government’s Infosec Standard 2 on risk management and accreditation of information systems

UK Government Cabinet Office advice on Information Risk Policy

New skills needed

All of those involved in risk management acknowledge that it is not easy, and that it is not a purely technical discipline. The information security professional (or more precisely, the information risk professional) needs strong personal qualities, including the ability to explain, persuade and negotiate with people at all levels of the organisation.

The language of risk provides IT

TABLE OF CONTENTS
EDITOR’S DESK
PERSPECTIVES
SCAN
FACE-OFF
RISK MANAGEMENT
GOVERNANCE
DISASTER RECOVERY
SPONSOR RESOURCES

and business with a common vocabulary that both can understand and employ. It also helps to inject interest and excitement into a subject that can often seem remote and boring to non-technical people.

"Risk management is not easy. It takes a lot of time and negotiation to be successful," says Marcus Alldrick, senior information risk and protection manager at Lloyd's of London. "That is why information security people need to be able to communicate. There are plenty of tools and methodologies around to help with risk management, but the real challenge is getting buy-in from the business and putting it into practice." ▸

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

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
FACE-OFF
RISK MANAGEMENT
GOVERNANCE
DISASTER RECOVERY
SPONSOR RESOURCES

5 ways security can influence VENDOR MANAGEMENT

BY ERIC HOLMQUIST

EVERY BUSINESS TODAY depends to some extent on third parties—it's a reality that's becoming even more pronounced as companies move to more cloud-based services. And in order to effectively provide a product or service, a certain percentage of those third parties will require access to confidential corporate and/or customer information. Obviously, it is incumbent on management to ensure that not only is the third party capable, but also in the course of its operations can ensure that the data entrusted to it remains secure. Traditional vendor management programmes have tended to focus to

THE CISO HAS A KEY ROLE IN REDUCING THE RISK OF SHARING SENSITIVE CORPORATE DATA WITH THIRD PARTIES.

a large degree on “ability to deliver” with data security being an almost secondary consideration. What managers often fail to fully appreciate, especially for large or very visible companies, is that while a third party’s failure to deliver would in all likelihood be operationally disruptive, a massive data breach could be devastating.

The challenge for companies is how to ensure protection when they often have little ability to monitor day-to-day operations, evaluate the third party’s strength of internal controls or have meaningful input into the third party’s risk management systems. While we often talk in terms of keeping the data “secure,” the grim reality is that, simply because people need to use it, the data is not secure. Adding an external entity into the equation just makes it that much less secure.

> The challenge for companies is how to ensure protection when they often have little ability to monitor day-to-day operations, evaluate the third party’s strength of internal controls or have meaningful input into the third party’s risk management systems.

Companies tend to approach vendor management in many different ways. Some split contract and vendor management between the legal department and other operating units, respectively. Some have large procurement groups that cover all aspects. Still others may use a decentralised model, distributing different pieces throughout the company. Regardless of which model is used (each having its own merits and drawbacks), the governance aspects related to data security really don’t change. We’ll explore five key risk management principles relative to information security within vendor management, and describe some basic strategies for reducing the risk associated with sharing confidential information. The CISO plays a key role by ensuring that the critical governance elements for data sharing with third parties are in place.

#1 ownership

The first and possibly most critical governance aspect is ownership. Regardless of how the contract and related due diligence is facilitated, one absolute and irrefutable truth remains: There must be one specific person responsible for the relationship—not a department, committee, or a vendor group—a person. In all likelihood, that person will be in the business or operating unit that directly oversees the product or service that the third party provides, be that IT, a line unit, back office, etc. This person, perhaps assisted by others, is specifically and directly responsible, and accountable, for management of that third party. This includes any damages caused by a failure of that third party to adequately protect the data provided to them.

Therefore, the first responsibility of the CISO is to make certain that the company has a process in place to ensure that each third party will have an associated third party relationship manager (TPRM) who is actively involved in the process of managing the relationship.

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
FACE-OFF
RISK MANAGEMENT
GOVERNANCE
DISASTER RECOVERY
SPONSOR RESOURCES

The CISO will likely end up being consulted in the due diligence process where appropriate, but he cannot be the one responsible for managing the third party.

While assigning a TPRM is essential, we need to understand that there is a dilemma here. Even though having TPRMs assigned to all third parties is critical to good governance, there is an unfortunate conflict of interest that exists here. The fact is, assuming that the business wants to use a given third party, the TPRM is somewhat less than motivated to find problems with them. In fact, quite the opposite; they may find themselves looking for reasons to trust the third party, perhaps ignoring subtle, or not so subtle, signs that could be an indication of something suspicious. This is why accountability is so critical—if TPRMs are responsible for the misdeeds of their third party, they become significantly less incented to turn a blind eye. Therefore, it is also the CISO's role to ensure that TPRMs are taking the contract, due diligence, management and monitoring process seriously and proactively.

#2 contractual provisions

Assuming clear ownership has been established, the next area covers a set of questions and provisions that the CISO must ensure are being addressed before any contracts are signed and data exchanged.

The first and most logical question is, why? Why does the third party need this data? Is it required for them to provide their product or service? Do they need all of the data or just some of it? Is the business area just being lazy and suggesting it all be sent, rather than taking the time to create more discrete, or sanitised, sub-sets? Ultimately, the related business area must be able to clearly rationalise why the data is imperative to the third party's product or service. This is an area where the CISO may be consulted as a subject matter expert, perhaps facilitating a discussion around what options exist that could reduce the type and quantity of data provided. It is a sad fact that well-meaning people often view data (even highly confidential data) as an operational necessity, like bricks to the builder, and not the highly valuable, highly sensitive, corporate asset that it is.

It is a sad fact that well meaning people often view data (even highly confidential data) as an operational necessity, like bricks to the builder, and not the highly valuable, highly sensitive, corporate asset that it is.

In terms of contractual provisions there are a number of things the CISO needs to ensure are included any time confidential data will be exchanged. These include:

- Standard confidentiality language commensurate with the degree of information shared
- A "right to audit" provision against the third party's system of internal controls
- Clear service-level agreements for notification requirements in the event of a data breach
- Financial liability for any expense associated with a data breach

In the end, however, a company needs to remember that while these provisions exist (at least in theory) to prevent an incident, the reality is that they largely exist for recourse. Real prevention will be accomplished through comprehensive due diligence, actively setting and managing expectations and effective monitoring.

#3 *due diligence*

All enterprises have skeletons they prefer not to disclose, so there's no reason to assume your vendors don't also have something they'd prefer to keep quiet. Consequently, the third major area that the CISO needs to be actively engaged in is the design of the overall due diligence process. The fact is that companies need to be very deliberate about how they assess and manage their third parties when it comes to data sharing.

When performing third-party due diligence, how the information is gathered isn't nearly as important as what is done with that information. (As far as forms go, you can't really beat the BITS Shared Assessment templates, and many major companies have already completed these forms anyway.) Generally speaking, the information provided by a third party relative to its information security practices should be viewed just like a resume. While it is a form of attestation on the part of the third party, it is not designed to verify adequacy; it's just a tool to start the conversation. The job of the organisation, with the CISO's direction and/or assistance, is to get behind all of the wonderfully crafted language and carefully constructed responses. What is the truth about how the third party stores, manages, protects and ultimately destroys the confidential data that you are, or will be, sharing? Where will it reside? Who exactly will have access? How is access granted and revoked? What are their change management practices? What technology is the third party using and does it contain known vulnerabilities? Is it current or obsolete? What independent reviews of the third party's environment are conducted and by who? What were the past results?

Generally speaking, the information provided by a third party relative to its information security practices should be viewed just like a resume.

This is not a check-off exercise—it's a gauntlet, and one that should be very difficult to navigate. If the business isn't asking really hard questions, it's not doing its job. It's the CISO's job to make sure that this process is happening, both at contract origination, and throughout the life of the contract.

Another part of the due diligence process should be a mechanism for classifying the data that will be shared. What type of information will be included? What is its level of sensitivity? How much information will be shared and how often, etc.? This provides a baseline for the business so that if the nature of the relationship changes, particularly one which requires a change to what data is shared, the company can reassess the risk based on the new data requirements. The CISO should be able to help develop an agreed-upon classification schema that can be used consistently throughout the organisation.

An area that is often overlooked is data destruction. When and how will the data be destroyed? How will the third party attest to its destruction and what are the consequences if it is not destroyed? This is a difficult area to manage because, let's face it, proving that data has been completely eliminated is difficult to impossible. Nevertheless, this area must be subject to clear expectations, which the CISO needs to ensure has been documented.

Ultimately, when going through the third party due diligence process, a company should develop a risk profile for all of its third parties that includes a risk rating based on the type and amount of the data being shared. This allows the company to focus its energy and resources on those third parties that represent the most risk, and provides a baseline to reference when either the third party or the nature of the contract changes.

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
FACE-OFF
RISK MANAGEMENT
GOVERNANCE
DISASTER RECOVERY
SPONSOR RESOURCES

#4 *monitoring*

Monitoring and incident response are the most challenging and precarious areas of vendor management. This is simply because monitoring is difficult if not impossible, and recovery from an event is extremely tough.

Nevertheless, despite the limited ability to monitor third parties, there are some areas that the CISO should ensure are addressed. The first represents internal changes. This would typically be a change to the scope of the contract which requires a change to the type, sensitivity, quantity or frequency of the data that is being exchanged. In this case, there must be a process to revisit the risk profile based on the new data requirements, and if a material change is going to take place, then a new due diligence and risk assessment analysis needs to be completed. Otherwise you're applying old rules to a new game.

Monitoring and incident response are the most challenging and precarious areas of vendor management.

The other area obviously involves changes with the third parties themselves. This would include facility moves, corporate restructuring, business acquisitions, new business lines, etc. Each of these can have an impact on the internal controls related to data protection, and it is the CISO's responsibility to ensure that systems are in place to monitor these third parties for material changes. Changes such as these should prompt, at minimum, a conversation between the TPRM and the third party to understand what impact, if any, these changes will have on the company's data usage and internal controls.

The other, and fairly intuitive, area of monitoring involves media coverage. Should the third party become subject to any degree of regulatory or other third-party criticism or, worse, be the victim of some sort of data compromise, then the entire due diligence and risk assessment process must start from scratch. All prior attestations and assumptions are

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
FACE-OFF
RISK MANAGEMENT
GOVERNANCE
DISASTER RECOVERY
SPONSOR RESOURCES

null and discarded.

The CISO will have to manage this area because this is where the TPRMs will often try to take the easy way out for fear of having to switch vendors. Often their response is "Yes, they had a breach, but they say that they have taken care of the vulnerability." O.K., prove it.

#5 *incident response*

Incident response is possibly the most treacherous part of vendor governance. Ideally, there will never be a scenario where data is compromised and somebody needs to clean up the mess. However, we know as a statistical certainty that it will happen and, when it does, the company needs to have the processes in place to respond quickly and decisively. The fact is that if you looked at every data breach since the beginning of time, they all share one common attribute—and that is that time is not on your side.

Certainly, at a minimum, every third-party contract must have a provision for notification requirement in the event of a data breach. This should be numbered in hours, if not minutes. On the heels of a data exposure, the initial hours can be critical, particularly where customer information is involved. CISOs need to ensure that both companies—their own and the third party—have a clear escalation and notification strategy so that all parties involved know exactly who needs to be notified and who will take charge in developing and implementing a resolution plan.

> On the heels of a data exposure, the initial hours can be critical, particularly where customer information is involved.

These are not details that can be made up at the time of a breach—they must be clearly established, and tested, well in advance of any live event. And, again, a data incident of any kind should prompt a revisit to the third party's due diligence and risk assessment. If the incident was very minor, very localised and easily corrected, fine. But at a bare minimum, a discussion needs to take place that asks whether the potential vulnerability was previously disclosed and how it has been addressed.

NO SMALL FEAT

Experience has shown that the majority of companies collect only basic information about the third parties with which they will exchange confidential data, tend to do only cursory analysis of that information, take minimal due diligence steps, implement limited monitoring and haven't really thought through their incident response procedures in the event of a major data breach. And yet every single one knows without a shadow of a doubt that it should be doing more and is probably accepting too much risk. Simply put, this is just not acceptable.

The CISO has a substantial task to ensure that all of the systems and controls are in place to ensure third-party compliance with information security policies and practices. To quote Ronald Reagan, this is definitely an exercise in “trust but verify” and it is no small task. This further reinforces why the CISO must be in a very senior role with total management access. He or she must work very closely with internal vendor management groups to provide subject matter expertise, programme design assistance and direct oversight when necessary. We all like to believe that people will always do the right thing, but this is simply not the case. There are criminals everywhere, and they can disguise themselves as hard working employees just looking for an opportunity to strike. But through strong contractual provisions, comprehensive due diligence, detailed documentation, active management, dynamic monitoring and ability to respond quickly, companies can go a long way towards managing their third-party risk.▸

Eric Holmquist is president of Holmquist Advisory, LLC, which provides consulting to the financial services industry in risk management, operations, information technology, information security and business continuity planning. Send comments on this article to feedback@infosecuritymag.com.

Safe Recovery

Security must be included in disaster recovery planning to ensure sensitive data is protected.

BY MARCIA SAVAGE

IN A DISASTER, all focus is—naturally—on getting critical business processes back up and running. Whether the disaster is natural or manmade, it's all about recovering business operations as fast as possible, getting employees back to work, and avoiding costly downtime.

In this scenario, information security is often far down on the list of considerations, experts say. But companies that overlook data protection provisions in their disaster recovery/business continuity plans risk winding up with a double whammy: a security breach on top of a recovery situation. Imagine having to issue breach notification letters in the midst of recovering from a hurricane or other disaster. After all, compliance requirements aren't lifted in an emergency.

"You need to get folks access to the data if they need it, but you also need to prevent unauthorised access," says Ed Moyle, a manager with CTG's information security solutions practice and a founding partner of consultancy SecurityCurve. "That's where a lot of organisations fall down."

Disaster recovery/business continuity plans must ensure that an organisation's information security policies are maintained in a recovery

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

FACE-OFF

RISK MANAGEMENT

GOVERNANCE

DISASTER RECOVERY

SPONSOR RESOURCES

situation, security practitioners and others say. That means making sure the recovery site has proper security, including updated antivirus and firewall protection. It also means conducting proper due diligence of any disaster recovery provider and taking proper precautions in a shared recovery facility. Transmission of data for backup purposes must also be secured.

"What you're doing to secure a disaster recovery site has to be every bit as good as what you're doing in your primary site," says Brian Engle, director of information security at Temple-Inland, a manufacturing firm based in Austin, Texas. "If you end up in a disaster recovery situation, it could be long term, maybe six months…Can you be comfortable with the decisions you make in choosing the facilities and the protections for that length of time?"

SECURITY LEFT OUT

Organisations often don't think about how the security controls they have during routine operation might fare in the event of downtime, Moyle says.

"For example, if you have a security programme built around the idea of keeping physical access to things like servers locked down, you may not be able to enforce that to the same degree in an emergency scenario as you could during normal business," he says. "You want to make sure security controls continue to function during a downtime scenario."

Some companies assign disaster recovery planning responsibilities to their security groups, but others focus on databases, servers and networks rather than security reviews in their planning, says William Hughes, director, consulting services BC/DR Center of Excellence at SunGard Availability Services. "They're not as involved as they should be," he says of security teams.

Organisations typically consider disaster recovery a business problem and often leave security out because they view security as an IT function that puts up barriers to business, says Randall Gamby, an enterprise security architect for a Fortune 500 insurance and finance company.

> "Security teams have insights into how data is protected and how access works. They need to be included."
>
> –RANDALL GAMBY, enterprise security architect for a Fortune 500 insurance and finance company

"Security teams have insights into how data is protected and how access works," he says. "They need to be included."

Security technologies are often considered overhead infrastructure, but if left out of disaster recovery/business continuity planning, could mean users can't access the business resources they need in a recovery situation, he says. For instance, if the organisation uses single sign-on in its routine business operations but SSO isn't supported in the disaster recovery plan, then users may not be given proper log-in prompts or be able to access certain back-end applications.

Some companies, however, make security a priority in their disaster recovery planning. An information security officer at a financial institution, who requests anonymity, says his organisation is in a highly regulated industry and cannot afford to overlook data security.

"Purely from the standpoint of being compliant with the regulatory bodies, it [security] has to be at the top of the list when we look at disaster recovery," he says.

COMPLIANCE CONSIDERATIONS

Indeed, companies—particularly those in highly regulated industries such as financial and health care—need to be aware that data security mandates aren't waived in a disaster.

"We have tremendous compliance requirements from a variety of regulators," says the financial information security officer. "The requirements for information security don't make a distinction between whether you're in a disaster recovery mode or not."

In fact, the HIPAA Security Rule specifically calls out the need for maintaining security in an outage situation, Moyle notes. Section 164.308(a)(7)(ii)(C) requires the implementation, as needed, of procedures to enable continuation of processes for "protection of the security of electronic protected health information while operating in emergency mode."

One disaster scenario to consider is the possibility of guard staff reductions and loss of monitoring capability to prevent theft, Moyle says. If servers or laptops are stolen with regulated data on them, a company would still have to meet breach disclosure requirements.

"You could incur regulatory penalties over and above what it costs you from a downtime standpoint," he says.

Organisations don't tend to get audited during a recovery operation but they need to be prepared down the road, SunGard's Hughes says. "Now I'm getting an audit six months later. How do I reconstruct the chain of custody for the data and how it was protected in the time frame, if the auditor wants that?" he asks.

Temple-Inland's Engle says he can't imagine a company that has PCI Data Security Standard compliance requirements deciding to operate for two months without protecting cardholder data after an outage. "You will get driven out of business if you go for an extended amount of time without all the same protections you had originally," he says.

"We have tremendous compliance requirements from a variety of regulators. The requirements for information security don't make a distinction between whether you're in a disaster recovery mode or not."

–An information security officer at a financial institution

RECOVERY SECURITY

There are a variety of disaster recovery methods including hot sites, cold sites, managed service provider and cloud-based services. No matter the method, organisations need to ensure the security of the site they're failing over to, experts say.

"You're trying to replicate normal operations at a backup site… Make sure you have all the security in place when you get there," says Beau Woods, solutions architect for security and risk consulting services at Atlanta-based security services

firm SecureWorks. That means making sure firewall protection, intrusion detection and antivirus are in place and updated, and if a company has a security operations center, making sure there's a place for those employees to sit, he says.

"You need to make sure that when people arrive to activate the site, that the controls in place are at least as strong as the controls that would be operating in a normal scenario," Moyle says. "The policy doesn't change in an emergency."

Gamby says companies often take it for granted that users have access to systems and forget about the access management layer—such as virtual directory services, federated technologies, and containment zones—that must be in place at the recovery site in order for business to continue.

"A lot of controls around data protection are based on a user's profile and that profile may get down to identifying the particular IP or MAC address for the system he or she uses," he says. "At a remote facility, you need to make sure those profiles are put in for those individuals so they can access the data from their desktops."

Organisations also need to consider encrypting the shared communication lines used for data transmission when switching over to a recovery site, Gamby says. After an incident, companies typically switch from their dedicated lines to a service provider's shared pipe to reroute traffic to the backup site. While the shared links won't mean cross contamination of data, someone managing the switching environment could look at the traffic crossing the lines, he says.

For BioWare, an electronic game developer, uptime and availability are critical—as is data security, says Craig Miller, senior team leader of infrastructure. The company uses a virtual tape library for disaster recovery; the digitally replicated tapes are sent over an encrypted VPN tunnel to another site. Every couple months, physical backup tapes are encrypted and sent to Iron Mountain.

"Being in game development, all we have is our data…If the assets aren't available or recoverable, we don't have anything," Miller says.

"Being in game development, all we have is our data…If the assets aren't available or recoverable, we don't have anything."

–CRAIG MILLER,
senior team leader of infrastructure, BioWare

BioWare uses two storage arrays from Compellent and plans next year to move one array offsite and double the disk size at each site for full cross replication; if one array goes down, the other could be active in seconds, he says.

VENDOR MANAGEMENT

If contracting with a fixed-site disaster recovery provider, managed service provider, or cloud-based service, companies need to vet them as they would any third party, says Rachel Dines, an analyst at Forrester Research.

"You need to know where they are storing the data, what are their encryption, access control and authentication policies, and whether they can provide documentation for all that," she says.

Organisations usually will ask vendors if they use encryption but neglect to ask important questions about the type of encryption, where the keys are stored and who has access to the keys,

TABLE OF CONTENTS

EDITOR'S DESK

PERSPECTIVES

SCAN

FACE-OFF

RISK MANAGEMENT

GOVERNANCE

DISASTER RECOVERY

SPONSOR RESOURCES

Missing Backup Tapes

A sample of breach reports involving backup tapes over the past two years.

October 2010
San Diego Regional Center, which serves people with developmental disabilities, notified some clients that a backup tape created for the purpose of disaster recovery testing was lost by UPS in shipping, according to a breach noticed obtained by PHIprivacy.net. The tape contained some current and former customers' names, Social Security numbers, addresses and medical diagnostic information.

September 2010
Pediatric and Adult Allergy, P.C., in Iowa reported losing a backup tape with patient personal information in July. Information on the backup tape included names, Social Security numbers and health plan data. The loss affected 19,222 individuals, according to the U.S. Department of Health and Human Services.

June 2010
Insurance broker Marsh and Mercer reported the loss of a backup tape that was being transported by a third-party courier, according to records obtained by DataBreaches.net. The tape contained employee benefits information; the data was maintained by Marsh's Association business, which operates through Seabury & Smith and Mercer Health & Benefits. The number of records exposed totaled 378,000, according to Privacy Rights Clearinghouse.

February & April 2008
Third-party couriers lose unencrypted backup storage tapes belonging to the Bank of New York Mellon in two separate incidents. The lost tapes potentially exposed the data of approximately 4.5 million people.

January 2008
GE Money, the firm hired by JC Penney to run its credit card operations, said it lost a backup tape containing the personal information of about 650,000 shoppers of JC Penney and other merchants. The tape was discovered missing in October 2007 by a worker at Iron Mountain.

—MARCIA SAVAGE

Dines says, adding, "Vendors shouldn't have access to your encryption keys."

Third-party recovery sites raise the issue of multi-tenancy, which brings additional security concerns, Dines says. "I'm not sure if people think through all the full implications of that—there are other companies' employees walking around there if they declare [an emergency] at the same time. You need to make sure the access controls to your infrastructure and data are strictly controlled."

SunGard's Hughes says customers in a shared recovery site need to step up their vigilance but acknowledged that can be a challenge. "That's tough in a recovery because that's not your first focus," he says. "The first is to get out of the situation you're in."

Cloud-based disaster recovery is relatively new but comes with a set of security concerns that organisations need to pay attention to, says George Ferguson, product marketing manager of security, compliance and continuity services at HP. The cloud-based option offers flexibility, cost savings and the ability to reduce recovery times, but companies need to step back and evaluate the cloud vendor's security controls, he says.

Ferguson cites the Cloud Security Alliance's guidance regarding the 13 critical areas of focus for cloud computing. Among the 13 areas is business continuity and disaster recovery, and the CSA recommends inspecting a cloud provider's recovery and continuity plans.

BACKUP DATA TRANSMISSION

Disaster recovery has traditionally relied on tape-based backup to off-site storage, but the transfer of those tapes doesn't always go as smoothly as organisations expect. In recent years, there have been numerous reports of backup tapes missing in transit, resulting in breach disclosures *(see p. 42)*.

Backup tapes are at risk in transit, but unlike BioWare, many companies still fail to secure them with encryption, experts say.

"We've come a long way in starting to secure devices like laptops, CDs and thumb drives, but when you look at the backup tape generated on a daily basis in a lot of organisations across the world…rarely is someone encrypting that," says Moyle.

SunGard's Hughes says companies tend to focus on the process of maintaining backup tapes and having a third party transfer them rather than securing them. He's seen a shift away from tape backups, not necessarily for security reasons but because of concerns with recovery times. At the same time, the cost of replication is going down, he said.

HP's Ferguson says the security risks of lost or stolen backup tapes—along with the need to improve recovery times—has driven a move toward electronic vaulting services, also called cloud-based backup and replication, as a means of avoiding the physical transfer of tapes.

Common Mistakes

Companies err in throwing disaster recovery planning onto IT and forgetting to test.

LEAVING SECURITY OUT is one of the mistakes organisations can make in disaster recovery/business continuity planning, but experts cite a couple other common mistakes: Leaving the planning to IT and not doing enough testing.

Companies often throw disaster recovery onto the IT team without prioritising what business functions are the most critical to recover and setting recovery deadlines, says Beau Woods, solutions architect for security and risk consulting services at Atlanta-based security services firm SecureWorks.

"IT has to make decisions on its own and it ends up not being in line with the business," he says. "You need to have a cross-functional group make those high-level decisions before going down the road of how you'll recover from a disaster and continue business."

Another frequent mistake organisations make is not conducting enough test of their recovery plans, Woods says: "You need to make sure the way you've designed it is the way it operates in real life, both on the technology and people/process side."

William Hughes, director, consulting services BC/DR Center of Excellence at SunGard Availability Services, also says testing is critical.

"People tend to build a solution and think that's the end state, but that's really just the beginning," he says. "The end state is about four tests later, after you work through the bugs."

—MARCIA SAVAGE

strategy

Overall, cloud computing has the potential to ease disaster recovery and business continuity by making it easier for organisations to have a mobile workforce, says Dean Ocampo, solutions strategy director at security supplier SafeNet.

"The benefit of moving to a cloud infrastructure is that you can access it from anywhere," he says. However, companies are reluctant to move their IT processes to the cloud until protections such as encryption and authentication are in place, he adds.

BUILT-IN SECURITY

Designing a disaster recovery site has to be similar to anything else—with security built in, says Temple-Inland's Engle.

For example, companies need to identify ahead of time potential areas where security controls constrain application functions or implementations and plan accordingly. If you know you had difficulties installing something in your primary environment then you should anticipate that it will be even more problematic in a recovery scenario. An organisation doesn't want to find itself in a situation where it's trying to recover an application and has to shut down security controls to make it work, and then is unable to turn them back on, he says

> "If you develop a disaster recovery plan and try to secure it on the back end, it's not going to work."
>
> –BRIAN ENGLE, Temple-Inland

"If you develop a disaster recovery plan and try to secure it on the back end, it's not going to work," he says.

The information security officer at the financial institution agrees that security must be integrated from the beginning.

"Our attitude is that we don't bolt on security—it's baked in across the board, not just for day-to-day operations but for that disaster recovery situation, which is potentially a day-to-day operation," he says.

Marcia Savage is editor of Information Security. *Send comments on this article to feedback@infosecuritymag.com.*

TABLE OF CONTENTS
EDITOR'S DESK
PERSPECTIVES
SCAN
FACE-OFF
RISK MANAGEMENT
GOVERNANCE
DISASTER RECOVERY
SPONSOR RESOURCES

TECHTARGET SECURITY MEDIA GROUP

INFORMATION SECURITY EUROPE

EDITORIAL DIRECTOR Michael S. Mimoso

SENIOR SITE EDITOR Eric Parizo

EDITOR Marcia Savage

MANAGING EDITOR Kara Gattine

NEWS DIRECTOR Robert Westervelt

SITE EDITOR Jane Wright

ASSOCIATE EDITOR Carolyn E.M. Gibney

ASSISTANT EDITOR Maggie Sullivan

ASSISTANT EDITOR Greg Smith

UK BUREAU CHIEF Ron Condon

ART & DESIGN
CREATIVE DIRECTOR Maureen Joyce

COLUMNISTS
Marcus Ranum, Bruce Schneier, Lee Kushner, Mike Murray

CONTRIBUTING EDITORS
Michael Cobb, Eric Cole, James C. Foster, Shon Harris, Richard Mackey Jr., Lisa Phifer, Ed Skoudis, Joel Snyder

TECHNICAL EDITORS
Greg Balaze, Brad Causey, Mike Chapple, Peter Giannacopoulos, Brent Huston, Phoram Mehta, Sandra Kay Miller, Gary Moser, David Strom, Steve Weil, Harris Weisman

USER ADVISORY BOARD
Phil Agcaoili, Cox Communications
Richard Bejtlich, GE
Seth Bromberger, Energy Sector Consortium
Chris Ipsen, State of Nevada
Diana Kelley, Security Curve
Nick Lewis, ACM
Rich Mogull, Securosis
Craig Shumard, CIGNA
Marc Sokol, Guardian Life
Gene Spafford, Purdue University
Tony Spinelli, Equifax

INFORMATION SECURITY DECISIONS
GENERAL MANAGER OF EVENTS Amy Cleary

VICE PRESIDENT/GROUP PUBLISHER Doug Olender

PUBLISHER Josh Garland

DIRECTOR OF PRODUCT MANAGEMENT Susan Shaver

DIRECTOR OF MARKETING Nick Dowd

SALES DIRECTOR Tom Click

CIRCULATION MANAGER Kate Sullivan

PROJECT MANAGER Elizabeth Lareau

PRODUCT MANAGEMENT & MARKETING Corey Strader, Andrew McHugh, Karina Rousseau

SALES REPRESENTATIVES
Eric Belcher ebelcher@techtarget.com
Patrick Eichmann peichmann@techtarget.com
Sean Flynn seflynn@techtarget.com
Jennifer Gebbie jgebbie@techtarget.com
Jaime Glynn jglynn@techtarget.com
Leah Paikin lpaikin@techtarget.com
Jeff Tonello jtonello@techtarget.com
Vanessa Tonello vtonello@techtarget.com
George Whetstone gwhetstone@techtarget.com
Nikki Wise nwise@techtarget.com

TECHTARGET INC.
CHIEF EXECUTIVE OFFICER Greg Strakosch

PRESIDENT Don Hawk

EXECUTIVE VICE PRESIDENT Kevin Beam

CHIEF FINANCIAL OFFICER Jeff Wakely

EUROPEAN DISTRIBUTION
Parkway Gordon
Phone 44-1491-875-386
www.parkway.co.uk

LIST RENTAL SERVICES
Julie Brown
Phone 781-657-1336
Fax 781-657-1100

COMING IN SUMMER

Data Protection: Keeping Data Safe With and Without the DPA

Following the issuance of the first Data Protection Act (DPA) breach fines, compliance with the regulation is more important than ever. But compliance alone will not necessarily protect organisations from a breach. This feature will focus on how organisations can keep data secure and pursue compliance.

Stuxnet, SCADA Security

Stuxnet put the spotlight on critical infrastructure protection, but will efforts to improve SCADA security come too late? This article will explore what it means to secure critical systems in an age of targeted malware, and the potential consequences of a security failure.

Client-Side Application Security

As widespread as Windows installations are, client-side applications such as Adobe Reader, Flash, Apple's QuickTime and others built on Java and AJAX code are more ubiquitous. This feature will look how enterprises can address these threats, manage security of client-side applications, and integrate fixes into existing vulnerability management programs.

Don't miss our quarterly columns and commentary.

TechTarget
Where Serious Technology Buyers Decide

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.

SPONSOR RESOURCES

IMPERVA®
Protecting the Data That Drives Business

See ad page 2

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

VERISIGN™

- Webinar: Managed DNS - Using Hybrid Routing to Optimise DNS Performance Resolution & Reliability
- Webinar: DDoS Defense - Augmenting your Business Continuity Practices in the Face of the Growing Threat
- Benchmark your Company's Infrastructure Protection: Take the Executive Threat Assessment

infosecurity®
EUROPE
19 – 21 April 2011
London, United Kingdom
www.infosec.co.uk

See ad page 4

- Infosecurity Europe TV
- Infosecurity Knowledge bank