MEDIA PLANET

No. 2/ August 2009

INFORMATION SECURITY

5 STEPS TO PROTECTING YOUR BUSINESS

KEEPING SAFE IN THE DIGITAL AGE

Under threat: Your business could be at serious risk if not aptly protected from online dangers and data leaks

PHOTO: VASILIY YAKOBCHUK

CHALLENGES

Cybercrime, like cyberspace, has no borders. As the modern world goes digital, it is essential for governments and businesses to put in place systems to **protect vital information,** and for politicians and corporations to think globally, and to put crucial networks to **guard against fraud in place.**

Why it is vital that information be made secure in the modern age

As a society we are shifting from analogue to digital networks at a sometimes frightening speed. Whether at work, at home or on the move we have all come to depend on digital technology in many walks of life.

For the most part this continues to have the potential to enrich our lives immeasurably. The internet, for example, is perhaps the first truly global network, connecting one third of humankind, and providing conversation and collaboration on an unprecedented scale.

But while the digital revolution offers a wealth of new opportunities for both businesses and individuals, it also brings unprecedented challenges and risks, not least in information security.

Online dangers

For the individual, most of the risks of the real world – short of physical harm – are replicated in the online world. Potentially harmful material can be created and disseminated, lies can be told, scams perpetrated, privacy invaded and the vulnerable led to harm themselves and others.

In business, almost across the board there has been a strong trend towards storing personal, important and sensitive information digitally. This increases speed and ease of access, which brings great benefits to the customer, but it can also make that data vulnerable to theft, unauthorised access and misuse. The consequences for a company if something goes wrong can be devastating, destroying trust among customers and leading to significant losses in revenue.

Outdated protection methods

Our frameworks for protecting information security have not kept pace with change. As a society we need to catch up. Cyberspace does not have borders. Issues relating to the governance of the internet are often outside the jurisdiction of individual governments. We need a global response to these security challenges. We cannot afford to make the mistake of taking our current systems and considering how we can adapt them to the online environment. Those countries that do will be left behind. We must evolve new models that reflect the global nature of the internet. As a Government, we recognise that to do this it will be vital to work with international partners as well as sectors across the UK.

The Government has recently announced our first strategy initiative to advance the security of cyberspace. On a national level we need to ensure that our networks are resilient enough to withstand and recover from deliberate attack and the impacts of problems such as severe weather. Later this year, a major test will be carried out to check the UK's ability to recover from a major loss of network capacity. We are also exploring the formation of a Tripartite Internet Crime and Security Initiative, bringing together parliamentarians, Government and business.

By its nature, the digital world is one where self-responsibility, self-regulation and international cooperation are crucial. But there is still a need for guidance and protection for individual users, businesses and national networks. By cooperating internationally and communicating effectively with businesses and individuals we hope to put the right framework in place to minimise the risks and maximise the opportunities a digital future will bring.

Pat McFadden
Minister for Business, Innovation and Skills, Department for Business, Innovation, Skills

MY BEST TIPS

Protect your data

1 Consumers must be able to communicate, trade, order services and work online with confidence. To do this the networks and services they use must be reliable. Securing their private data against misuse or fraud is essential.

Be prepared

2 Service providers must respond quickly to instances of fraud and to fix any vulnerabilities that are discovered. Suppliers must make their products more secure against digital threats.

WE RECOMMEND

Protect your business
A proactive guide to protecting your business from cyber threats
PAGE 12

"When a vendor makes a patch public, this is akin to telling the world there is a weakness in their software."

MEDIA PLANET
We make our readers succeed!

INFORMATION SECURITY, 2ND EDITION, AUGUST 2009

Editorial Manager: Katherine Woodley
Sub-editor: Danielle Stagg

Project Manager: James Sheerin
Phone: +44 (0)207 6654403
E-mail: james.sheerin@mediaplanet.com

Distributed with: The Daily Telegraph, August 2009
Print: Telegraph Media Group

Mediaplanet contact information:
Darren Clarke
Phone: 020766544014
Fax: 02076654419
E-mail: darren.clarke@mediaplanet.com

ANATOMY OF A DATA BREACH

WHY BREACHES HAPPEN AND WHAT TO DO ABOUT IT

For companies with critical information assets such as customer data, intellectual property, trade secrets, and proprietary corporate data, the risk of a data breach is now higher than ever before. Global operations with outsourced and off-shored business functions spread the vulnerability.

Tools for accessing and distributing information, such as the Internet and mobile computing devices, exacerbate the risk. It should come as no surprise that more electronic records were breached in 2008 than in the previous four years combined. [1]

In a world where data is everywhere, it has become harder than ever for organisations to protect confidential information. Complex, heterogeneous IT environments make data protection and threat response very difficult.

Yet today's businesses depend upon their security teams to ensure that information collaboration and sharing by an increasingly mobile workforce remains safe and secure.

Information vulnerability and risk come from both malicious and unintentional disclosures by employees and partners; with unintentional disclosures usually the larger problem. Reducing these risks and vulnerabilities is now both a business imperative and a legal mandate as regulations impose obligations on organisations to protect certain types of information.

WHY DATA BREACHES HAPPEN

While the continuing onslaught of data breaches is well-documented, what is far less understood is why data breaches happen and what can be done to prevent them.

In order to get ahead of the data breach challenge, it is essential to understand why they occur. Third-party research into the root causes of data breaches, including data from the Verizon Business Risk Team[2] and the Open Security Foundation[3], reveals three main types: well-meaning insiders, targeted attacks and malicious insiders.

In many cases, breaches are caused by a combination of these factors. For example, targeted attacks are often enabled inadvertently by well-meaning insiders when an insider's failure to comply with security policies leads to a breach[4].

Well-Meaning Insiders. Company employees who inadvertently violate data security policies continue to represent a major factor in occurrence of data breaches. According to the Verizon report, 67% of breaches in 2008 were aided by "significant errors" on the part of well-meaning insiders[5]. In a 2008 survey of 43 organisations that had experienced a data breach, the Ponemon Institute found that over 88% of all cases involved incidents resulting from negligence[6].

Targeted Attacks. In today's connected world, where data is everywhere and the perimeter can be anywhere, protecting information assets from sophisticated hacking techniques is an extremely difficult challenge.

Driven by the rising tide of organized cyber-crime, targeted attacks are increasingly aimed at stealing information for the purpose of identity theft. More than 90 percent of records breached in 2008 involved groups identified by law enforcement as organized crime[7]. Such attacks are often automated using malicious code that can penetrate into an organisation undetected and export data to hacker sites.

In 2008, Symantec created more than 1.6 million new malicious code signatures, more than in the last 17 years combined, and blocked an average of more than 245 million attempted malicious code attacks worldwide every month[8].

The Malicious Insider. Malicious insiders constitute a growing segment of breach drivers, and a proportionately greater portion of the cost to business of data breaches. The Ponemon study found that data breaches involving negligence cost $199 per record while those caused by malicious acts cost $225 per record [9]. With the steady drumbeat of data breaches making headlines almost daily, it might seem reasonable to regard data breaches as an inevitable by-product of our connected world, a cost of doing business that we must simply learn to live with.

A closer view of the facts, however, suggests that this is not necessarily the case. Symantec's security expertise, global intelligence network and real-world experience with customers combine to inform a more confident perspective.

By following a risk-based and content-aware information security strategy that incorporates multiple solutions working together in concert, data breaches are preventable.

HOW TO STOP DATA BREACHES

To monitor and protect information from both internal and external threats across every tier of their IT infrastructure, organisations should select solutions based on an operational model for security that is risk-based, content-aware, responsive to threats in real time and workflow-driven to automate data security processes.

Here are six steps that any organisation can take to significantly reduce the risk of a data breach using proven solutions:

1. Proactively protect information with a unified data loss prevention solution.

2. Automate the review of entitlements to sensitive data.

3. Identify threats by correlating real- time alerts with global security intelligence.

4. Deploy a multi-layered combination of security solutions to stop incursion by targeted attacks.

5. Establish network defenses to detect and block data exfiltration.

6. Integrate prevention and response strategies into security operations.

HOW TO GET STARTED

Global corporations and government organisations require more than network security and access control to guard their confidential data. They must protect the information itself, inform the behavior of those carrying the information, have visibility regarding where their confidential data resides on their network, have influence over where that data is going and implement a policy for managing it.

It is vital for organisations to devise a strategy that balances their legal and business obligation to protect information with the competing need to share that same information.

By combining industry-leading advisory consulting services and data loss prevention technologies, Symantec is uniquely positioned to provide customers with not only a detailed analysis of their data breach risk, but also a quantitative assessment of actual data loss risk across networks, web applications, storage and endpoints.

To get started, contact Symantec at **www.symantec.co.uk/dlp** to schedule a Data Breach Workshop with one of Symantec's data loss prevention experts.

ABOUT SYMANTEC

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organisations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at **www.symantec.co.uk/dlp**

This advertorial is an extract of the full Anatomy of a Data Breach whitepaper. To access a full copy of the whitepaper, go to **www.symantec.co.uk/dlp**

symantec™

1 Verizon Business Risk Team, 2009 Data Breach Investigations Report. 2 Ibid. 3 http://datalossdb.org/ 4 Verizon Business Risk Team, op.cit. 5 Ibid. 6 Ponemon Institute, 2008 Annual Study: Cost of a Data Breach, February 2009. 7 Ibid. 8 Symantec Internet Security Threat Report XIV. 9 Ponemon Institute, op. cit.

NEWS

STEP 1 TAKE IT SERIOUSLY

CYBERCRIME BIGGER THAN DRUGS TRADE

Question: What is the scale of global cybercrime, should companies and consumers be concerned?

Answer It is hard to gauge but latest research suggests huge profits and low risk are encouraging criminals to steal corporate secrets as well as bank and credit card details.

Although it may sound like an alarmist finding, a cybercrime author's recent research is suggesting the long-held fear that cybercrime would overtake drug smuggling has come true.

Guillaume Lovet, whose Dirty Money on the Wires research is available online, admits it is almost impossible to put a figure on global cybercrime and believes predictions it is a trillion dollar industry are probably overblown.

However, he certainly feels it nets organised crime gangs far more than the £100bn drug trade for some very simple reasons.

Many layers

"It's like an onion with many layers and often the different people involved don't know each other, so catching anyone is difficult catching everyone involved in a crime is virtually impossible," he says.

"You have the guys who discover vulnerabilities, the guys who can then use these vulnerabilities, those who host them and then the organised crime bosses at the top who know how to turn the data and access to bank accounts in to real money elsewhere."

The latter role is the most challenging and Lovet reveals he recently eavesdropped on a secret online auction for access to a bank account containing $200,000 which was sold for just $300.

The disparity is due to only top criminals being able to launder money successfully, giving them a huge return. "The profit from this is extraordinarily high and the risk of getting caught is almost nil," he says. "It's a similar profit margin from drugs but those guys shoot each other and get caught by the authorities, it's very risky.

Guillaume Lovet "it's very easy for the cybercriminals to get away with it. Not only is it very hard to catch them but it's very rare that the crimes actually get reported."

With cybercrime they use the 'onion' method. When they sell on a vulnerability to the next person they go through many layers of servers so nobody can trace anyone else. So, nobody knows who they're working with and so nobody can catch them."

Unreported crimes

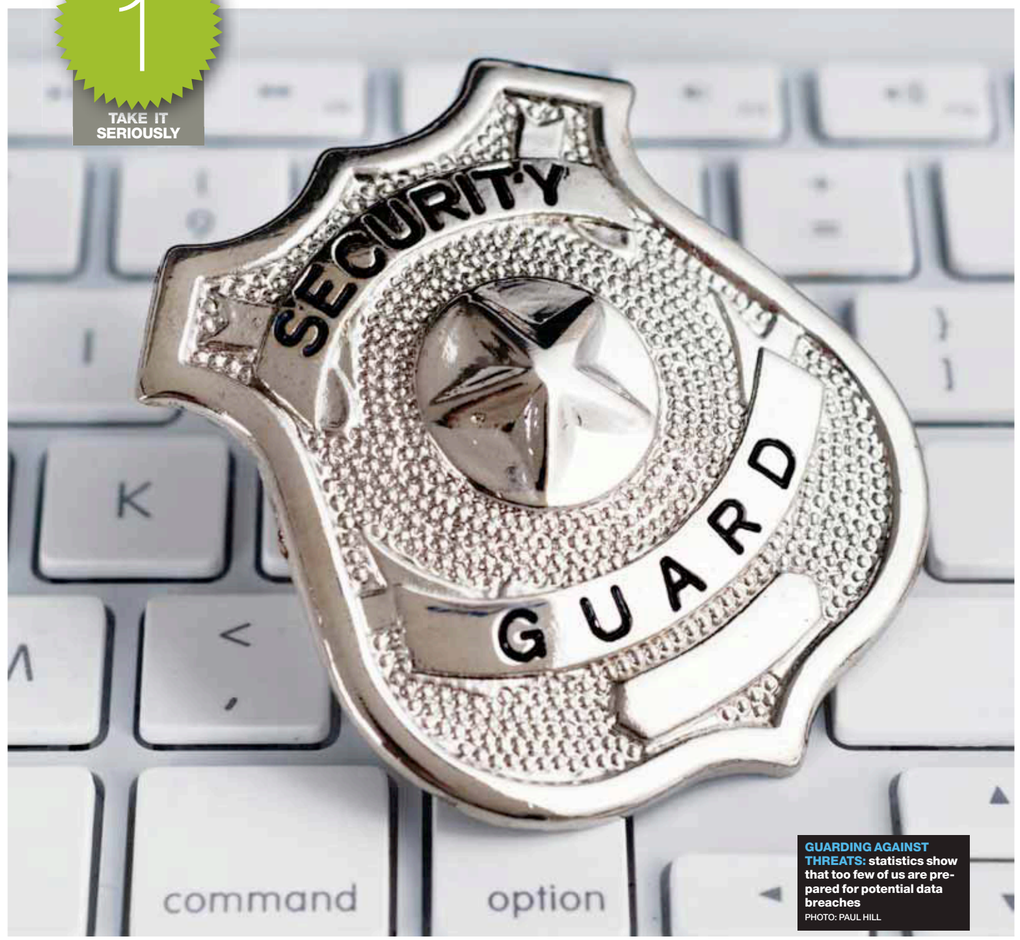
It may sound odd but Lovet maintains that the main reason why cybercrime is so successful is that, at a corporate level, it is very rarely reported.

"Individuals will report their credit card or bank account being abused but companies are too embarrassed," he says. "So, it's very easy for the cybercriminals to get away with it.

Not only is it very hard to catch them but it's very rare that the crimes actually get reported in the first place."

Hence Lovet's advice is for companies to 'patch' software as vulnerabilities are reported as well as use up-to-date cyber security systems and educate staff of the dangers of lapse information security practices.

SEAN HARGRAVE
sean.hargrave@mediaplanet.com



GUARDING AGAINST THREATS: statistics show that too few of us are prepared for potential data breaches
PHOTO: PAUL HILL

Reputation, compensation and fines: The cost of data leaks

NEWS

Twitter. A hack attack has left the web sensation embarrassed and calling in its lawyers

One of the biggest names in social networking and blogging, Twitter, has ironically become the latest household names to suffer a leak of sensitive data.

The embarrassed micro-blogging site is claiming that no user information was lost when thieves stole sensitive documents belonging to one of its workers.

Nevertheless, the fact that one of the most well known online businesses could be hacked will do little to create user confidence. The episode was exacerbated by at least one well known web site leaking outline details of the stolen data, which was claimed to include sensitive financial predictions, details of meetings and lists of senior people employed at rival companies who had applied for executive level jobs at Twitter.

The result has been an embarrassing admission of a breach, combined with the likelihood a spat with one of the most respected news sites in its field will result in costly legal action.

Expensive threat

Data leaks are not just embarrassing; they can often be very costly.

The worst ever case, two years ago, saw hackers getting an estimated 45m to 95m credit card details by simply sitting in a car park with a wireless laptop computer outside a TJX store. The American retailer had to set aside $118m to compensate victims and secure its networks. Two years on, its name will still always be synonymous with the scandal.

The threats are not only from hackers. Regulators are getting tough too. The FSA fined HSBC £3m for lapse security this July. The financial regulator criticised the banks for losing discs containing unencrypted information on 182,000 customers.

In fact, financial institutions are top of the list of high risk businesses which researchers at IDC have warned could have sensitive data stolen despite use fibre optic networks.

These have been viewed as secure but the researchers are warning companies they still need to ensure optical networks are fully protected and data held within systems is encrypted.

NEWS

Staff training key for data security

Technology can help prevent data leaks but is not a 'silver bullet' warns William Beer, Director of PwC's OneSecurity Team. He advises staff training is as critical as installing the latest technology. "You've got to teach staff about data security and have it engrained in them," he says.

"They need to know it's not ok to leave work laptops in the boot of a car that could be stolen, even if the contents are encrypted because losing brand reputation is as damaging as losing sensitive data.

"Companies which start to teach awareness notice fewer serious incidents happening but also get a lot more minor incidents pointed out to them as staff realise the importance of vigilance, particularly among new recruits and people about to leave the company, as well as third parties, such as outsourced staff."

SEAN HARGRAVE
sean.hargrave@mediaplanet.com

NEWS


1

2


3

STEP 2 KNOW YOUR ENEMY

SECURING YOUR PC
1. The damage a virus can cause on your computer -and business- can run deep
2. Statistics show viruses are being engineered to attack our data
3. The anonymity of the web means you can no longer be sure who is accessing your informtation
PHOTOS: ISTOCKPHOTO

Viruses evolving to steal rather than destroy

Question: Do viruses still 'eat' data and cause a nuisance on a PC, or have they evolved?
Answer: Viruses are totally different and far more dangerous today. They're not as openly destructive but instead aim to sit undetected on a PC stealing a user's personal information.

SHOWCASE

Just a handful of years ago viruses were very different and posed far less of a threat than today. Virus writers used to prove their 'skill' through destructive code which would wipe hard drives and cause havoc and put their nickname, often embedded in code, in the headlines.

Today, though, organised crime is involved and looking to make money from viruses and so the code writers which supply them with malware craft programmes whose aim is to do nothing openly destructive. Instead, they are designed to secretly sit on a computer and 'keylog' passwords as they are entered on sensitive sites, such as financial institutions, so identities can be falsified and accounts bled dry remotely.

As Howard Schmidt, President of the Information Security Forum points out, this marks a signal shift in the intent behind virus attacks and underlines the need for companies and individuals to protect themselves.

"Today, it's all about money, nobody's trying to show you how clever they are, they just want to steal from you without you noticing."

Howard Schmidt
iSF President

While the names of the various viruses will change, the motive of monetary gain remains constant. "Things have changed since malware like the famous Kournikova virus deleted files and caused a nuisance," he says. "They've evolved to steal credit card and bank details as well as turn machines in to 'spambots' which send out endless spam from the computer owner's email account. Today, it's all about money, nobody's trying to show you how clever they are, they just want to steal from you without you noticing."

While most viruses are aimed at providing criminals with access to a bank or credit card account, some will also look for sensitive information on corporate systems which criminals know they can then sell on to rivals or use to embarrass the victim company. Hence, while Schmidt, a former White House security advisor, advises people not to panic, because the vast majority of web traffic and emails are perfectly legitimate, he does urge companies and individuals to ensure their firewalls and anti-virus products are up to date and that patches for flaws in programmes (which hackers can use to penetrate systems) are implemented as soon as possible.

It is for this need for all-round protection that many companies are now switching to Unified Threat Management (UTM) systems which combine spam filters, firewalls, anti-virus and intrusion prevention capabilities in a single device at the gateway of a company's network. A recent study by Aberdeen Group researchers shows those opting for a UTM approach saw a 20 per cent drop in threat or vulnerability related incidents.

FACTS

- Almost nine in every ten emails are spam (compared to three in four last year).
- One in every 295 emails contained a virus (down from one in 148 for July 2008).
- 3,394 new malicious websites discovered and blocked every day (up 50% year on year).
- One in every 327 emails contained a phishing attack (down from one in 180).
- 3.6m 'bots' traced – these are computers being remotely controlled, typically to send out spam.
- 85% of all spam traced back to networks of 'bots' called 'botnets'.
- 'SOBIG' the largest 'botnet' of the year behind one in every 17 emails.
- One in every 78 web address included in Instant Messenger programmes is malicious.
- 60 attempts at corporate espionage and spying detected every day. This had risen to 100 per day during the G8 summit.
- 100m visits made to malicious web sites made every month.

QUESTION & ANSWER

RODNEY JOFFE
A founding member of the Conficker Working Group reveals the full horror of the most successful worm ever to be released.

NO CURE YET FOR SOPHISTICATED ATTACK

What is Conficker and why should people be worried about it?

! "It's the most effective worm ever launched which we believe is currently infecting around five million computers. It opens up computers to a whole host of viruses and malware attacks. It's not dangerous in itself, it's the fact it opens up a computer to all manner of attacks.

The most worrying thing is this was discovered last autumn and we still can't beat it. There's no cure for it and it has been released in different incarnations to get around measures taken to try to defeat it."

How does a PC get infected?

! "One of the worrying things is your PC can get infected without you doing anything. It's mainly being moved from one machine to another by infected USB stick drives and CDs but it can also spread around the net. It uses a vulnerability found in Microsoft's software which, before it was patched, left a port open on computers through which the worm can gain access."

What's clever about the code?

! "Conficker is amazing. It uses encryption technology which is so state of the art nobody knows how to decrypt it. If I were a professor and the bad guys who wrote this showed me it I would have to give them an A+. It's the most sophisticated worm anyone has ever seen..."

What can be done about it?

! The best advice is to keep your Windows software set to automatic updates and ensure your anti virus software is up to date. If a machine is infected, the only solution is to wipe its hard drive completely and load all the software on it again with fresh disks from the suppliers.

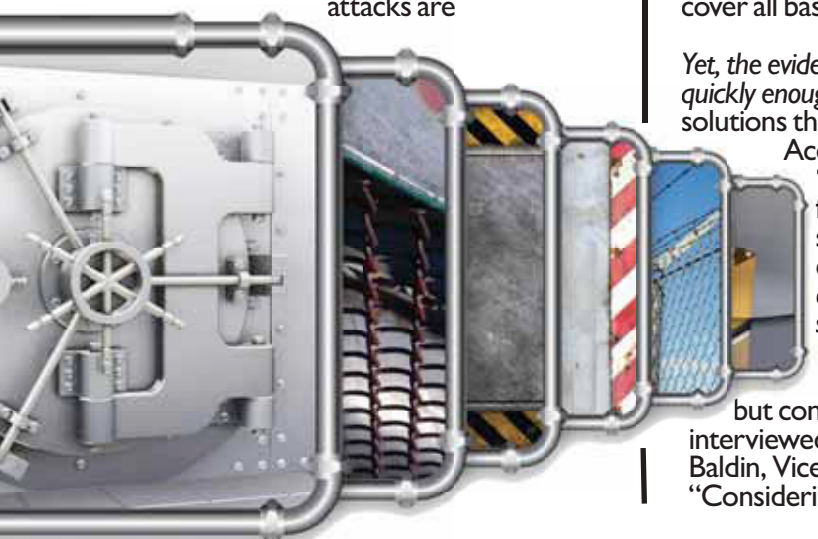
Computers can be tested for infection by clicking on the supplied 'test' link at www.conficker workinggroup.org

Securing each part of the enterprise

Workers want the freedom to roam, but flexible working practices plus a new generation of security threats are demanding a layered approach from enterprises.

Businesses, it seems, are happily embracing the freedom afforded by mobility. In fact, research group *IDC estimates that by 2013 30% of the total global workforce will be mobile workers.* But mobility is just one issue demanding a change in the way enterprises handle security. The days of the lone hacker are long gone. Businesses are now facing attacks that are targeted, organised and highly malicious and are generally using the web and mobile devices to reach the network.

Several patterns are emerging. Attackers no longer able to get in through the operating system are targeting individual applications, and these attacks are largely coming from the web in a way that avoids signature-based security. Malware, such as Trojans, keyloggers, spyware and rootkits, are becoming more common and these attacks are now organised by large, multinational syndicates hoping to get to personal data and corporate intellectual property.



In the fight to maintain a secure network perimeter, mobility is an added complication. Laptops used outside the firewall, plus other devices such as USB drives, increase the opportunity to penetrate. They also add to the headaches suffered by the IT Manager, who has to ensure security on these devices is constantly updated when network topography is changing. Organisations must ensure that sensitive company data is protected with the most advanced solutions available, by implementing a proactive "layered" security strategy. Taking a layered approach means that enterprises need to both expand and consolidate their security efforts to cover all bases.

Yet, the evidence is that enterprises are not responding quickly enough, and aren't completely aware of the solutions that can fight modern security threats. According to the 2009 IDC report 'Endpoint security: A Timely Warning for Today's Economic Climate', which surveyed enterprises of over 2,000 employees, *only 76% of businesses are adopting the kind of layered approach to security that can deal with the proliferation of attacks.*

This may seem like a good proportion, but considering the size of the businesses interviewed, the figure should be higher. Says Andy Baldin, Vice President, EMEA, Avocent LANDesk: "Considering the new reality of the network and the complexity of the threats involved, a layered approach to security should be the base point rather than an aspiration for all enterprises. Businesses have to act now; they can't afford to leave this unaddressed."

Perhaps a barrier to adopting layered security is the fear that point products are too difficult to manage; especially in light of the increased sophistication of the security threat. IDC predicts that businesses will increasingly turn to vendors offering a single, integrated endpoint solution which can manage all the tasks handled by individual products.

Andy Baldin adds, "An integrated endpoint security solution ultimately improves the life of an IT Manager by increasing the ease of manageability, minimising risk to the endpoint and reducing costs".

Companies, not having done so already, should look to implement a centralised layered endpoint security strategy that can react to the most pressing threats as they change over time, and can be built around the needs and the structure of the network and the business. Anything less is leaving security to chance.

Find out more at http://secureit.landesk.com/

Avocent | LANDesk

STEP 3 BE CAREFUL

Question: What is the biggest information security threat for me and my business?
Answer: History would suggest poor security practice is a significant issue for businesses

For the biggest source of risk, look in the mirror

CHANGE

You can have the best software in the world, but that still won't guard against human error. People, not products, are the biggest security risk of all.

Roger Southgate is a past president of ISACA (Information Systems Audit and Control Association) and is now an independent governance and risk consultant. Based in Portsmouth, Roger started his career in accountancy and moved into IT in 1980, going on to become the CIO of a Japanese investment bank. He is adamant that the biggest risk of all to a company's security is simple - it's people.

"In many cases, companies don't practice what they preach," he says. "Banks and other companies take a procedural rather than a professional approach - in other words, they train employees to follow a procedure, but those employees don't understand why they have to do it. So when things go wrong, they don't understand the cause."

The most fundamental problem, according to Southgate, is that security is seen as a stand alone area to be added on rather than fundamental to a company's set-up. "It's seen as a technical area, rather than something to be embedded in the fabric of an organisation," he says. "People simply don't understand the security implications of what they're doing."

Human error can occur on every level. Southgate cites one very common scenario: the reaction to a systems breakdown. "In most companies, time is money and getting the system working again is crucial," he says. "If they can't get a system working immediately, the first thing a technician does is to dismantle the security. Then they don't revisit to make sure it's in force and operational."

Another hugely common problem is the loss of a laptop, a CD or a hard disc, as has happened countless times in recent years. "Software is very good now," says Southgate. "But equipping employees with this equipment is like giving them a Ferrari and not teaching them how to drive." There is no simple solution to this: you can not guard against someone losing their laptop. You can only control what is on it and even then people download information they shouldn't - say, sales targets - and take it out of the office.

"Equipping employees with this equipment is like giving them a Ferrari and not teaching them how to drive"

Roger Southgate
Former ISACA president

Organisations are increasingly sharing data, which causes more problems as secure data, such as credit applications, are passed from hand to hand. Then there is the issue of when someone is promoted within a business or leaves it all together. "No one has cracked what to do when people change their roles within an organisation," Southgate says. "They will frequently end up with two user profiles, doubling the chance of making a mistake. Companies are poor at disabling and removing users when they leave."

Then there are issues that can seem harmless, such as giving a colleague your password. "There's very rarely malicious intent behind it, but people do make mistakes."

Southgate himself was horrified about a year ago when he was sitting in a coffee shop: the man next to him, who was using wireless, asked him to keep an eye of his computer while he went to get another drink. The fact that younger employees are also now used to constant, free access to the internet via lap tops and mobiles also causes problems. "They have no difficulty liaising and talking to friends in the workplace, which may mean they are opening up their organisation's resources to someone new. You have to strike a very delicate balance," he says.

ISACA runs sessions to teach how to guard against all these cases of human error, while Southgate himself acts as a consultant to companies fearing or experiencing problems. "I physically have to get the attention of the right people, and make them understand that technology alone won't solve the problem," he says.

"Security is like an onion: there are layers and layers to peel back. You need fundamental controls built deep into the business process. Only then can you have a hope of breaking through."

VIRGINIA BLACKBURN
virginia.blackburn@mediaplanet.com

SELF- MONITORING
By eliminating human error you can minimise the risk of data breaches
PHOTO: MANUELA KRAUSE

4
ROGER'S BEST TIPS

Know your system

1 Understand their fundamental security model. There are basically two: to secure everything and grant permission to access it selectively, or grant permission for access to everything and secure selectively. Understand why you are using the security you are doing and make sure your staff understand it, too.

Be in-the-know

2 You can never have enough security awareness and training. There should be a senior member in staff in charge of security, and it should be accepted as a fundamental part of the business.

Take it seriously

3 Sell the importance of security to your workforce on the basis of the benefit it provides to customers. Make them take a reality check: what would they do if this happened to them?

Keep it up

4 Be patient, be persistent. And make sure you and your staff are totally up-to-date.

PHOTO: TATIANA POPOVA

INSPIRATION

KEEP IT SAFE
Your business may be unprotected from the little-known threats which devastate companies everyday
PHOTO: NICK SCHLAX

Keeping your paperwork safe

■ **Question:** How can I keep my information safe from the threat of data loss or security breaches?

■ **Answer:** By being pragmatic and considering specialist help, your business is more likely to be protected.

CHANGE

It is not just company premises that need protecting: it is the information kept, quite literally, on paper within a company that needs to be looked after, too.

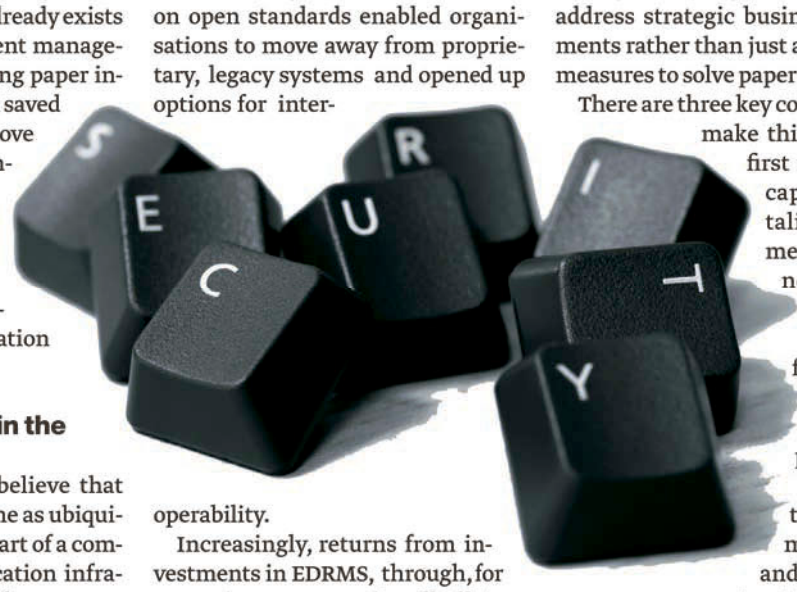
Some of the major UK software security companies have developed an Electronic Document and Records Management System (EDRMS) as a key component of the wider Enterprise Content Management (ECM) framework, which helps deal with web content management, document and records management, electronic forms, business process management, collaboration and compliance processes.

ECM is essentially a conceptual framework for centralised information access, creation, management, and standardisation of business processes. There is no magic bullet solution - just a common sense approach which focuses the available technologies on specific business processes to ensure that the solution delivers what is expected of it.

Experts in the industry describe this as essentially a "migratory" process: new documents are "born" into the repository, while legacy information - that which already exists - is scanned in. Document management started with turning paper into electronic files, which saved space and was easy to move around and share; increasingly sophisticated Electronic Document Management Systems (EDMS) can now also support systems integration, workflow, collaboration and compliance

Integrated role within the company

Many companies now believe that EDRMS is likely to become as ubiquitous and as pervasive a part of a company's enterprise application infrastructure in the coming few years as database management systems have been over the past two decades. Database management systems based on open standards enabled organisations to move away from proprietary, legacy systems and opened up options for interoperability.



Increasingly, returns from investments in EDRMS, through, for example, process and staff efficiencies, standardisation, automation via workflow and so on are coming through via using the technology to address strategic business requirements rather than just as short term measures to solve paper problems.

There are three key components to make this work. The first is document capture: digitalising documents alone is not enough. The solution must offer facilities to stop producing new paper.

Secondly, there must be management and systems integration, in which content must be integrated with core business systems and practices. This involves day-to-day management, along with compliance and issues concerning external threats, such as malicious damage, fire, flooding, theft and so on.

And finally, delivery: there must be access to key users as and when they need it. These new systems are making real changes, from hospital wards to local planning and beyond.

VIRGINIA BLACKBURN
virginia.blackbutn@mediaplanet.com

FACTS

There are a number of software solutions that can help in document management. To help you choose, you need to know these useful terms:

- Electronic document capture (EDC) - this utilises scanning, text recognition and image conversion
- Optical character recognition (OCR) - the mechanical or electronic translation of images of handwritten, typewritten or printed text (usually captured by a scanner) into machine-editable text
- Electronic document management system (EDMS) - the overall system containing the documents: it can range from the very simple to the very complex
- Electronic record management system (ERMS) - this is particularly suitable for, say, payrolls and patient records
- Web content management (WCM) - for managing websites
- Workflow management (WFM)
- Knowledge management (KM)

Keeping watch
One of the 14,000 employed by protective services

A global phenomenon

In recent years is becoming increasingly acceptable for governments to turn to security companies for help with public and national security issues.

Security companies now operate all over the world. One of the largest of these is GTZ, or the Deutsche Gesellschaft für Technische Zusammenarbeit GmbH, based in Eschborn, near Frankfurt am Mein. It does a great deal of work for the German government, as well as the European Commission, the United Nations, the World Bank and numerous private companies. The company now operates in 130 countries in Africa, Asia, Latin America, Eastern Europe and the New Independent States, employing more than 14,000 staff.

Back in Britain, the largest security group is G4S, formerly Group 4 Falck A/S, before its 2004 merger with Securicor, also the biggest security group in the world. The company works in over 110 countries throughout the world, with an excess of 585,000 employees. Its business goes far beyond what is traditionally seen as standard security provision: in 2008, for example, it acquired RONCO Consulting Corporation, which is a humanitarian commercial mine action, ordinance disposal and security companies. It undertakes virtually every type of security work, including guarding major events such as Wimbledon.

Of course, Iraq provides the greatest opportunity for private security companies at the moment, especially as the situation stabilises and rebuilding the country continues apace.

There are over 40 PSCs out there, so many that the Private Security Company Association of Iraq has been created to consider matters of "mutual interest and concern": it meets about every three weeks inside the International Zone in Bagdad, meetings also attended by other interested bodies such as the Iraqi Ministry of the Interior, the US Embassy Regional Security Office an and Joint Area SupportGroup Central (JASG-C) Security irectorate.

WHAT IS THE REAL COST TO YOUR BUSINESS?

Virus is a small word, but a powerful one. Most of us understand the connection with world events and our own health, think Swine Flu, but it's often much harder to understand the complexities of loss when assigned to our business computers and networks.

What can a virus do to your system? Well imagine everything going up in a proverbial puff of smoke, all your emails moved to the delete folder without having moved a finger. No contracts, no invoices, no HR data, no payroll. Everything has simply vanished. Your business is literally ground to a holt while you try to piece back together the systems that have taken you all that precious time to develop. The impact of such a loss has far reaching implications many businesses aren't taking into account. Your reputation, your future earnings, your supplier relationships all can be effected by a simple and relatively small thing called a virus. Amazing what power that word really has.

To put the risk in perspective, it took 20 years for about 250,000 viruses to be developed but between 2007 and 2008, there was an estimated 1.3million viruses lurking to attack your systems, and the figure is set to grow exponentially.

At a time where businesses are all struggling with limited resources and opportunities, this is not the time to let one of those small but devastating viruses sneak in. And this isn't just a concern for multi-national organisations, small local home office users are just as exposed and the consequences just as severe. Security threats are becoming more varied and complex every day and targeted attacks to all businesses are on the rise.

There is no reason for any business to put their existence at peril when simple steps can be taken to secure and cope with the threat.

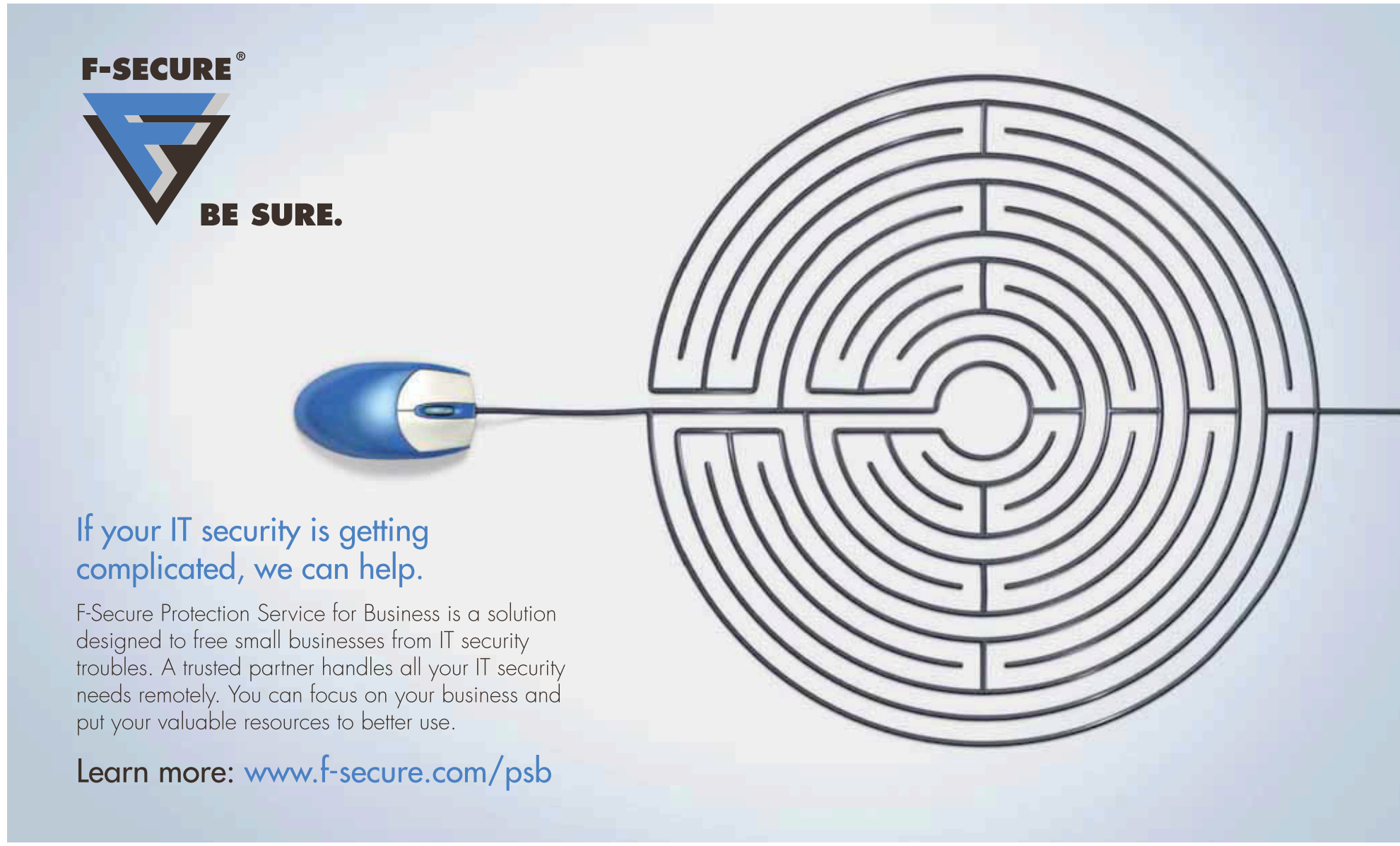
Security as a service is the way forward for businesses. It allows you to maintain focus on your core business rather than becoming a security or virus expert. Instead of buying lots of different anti-virus products, subscribe to a protection service and let the security vendor do the work.

F-Secure offer a security service that is easy to deploy, use, manage and maintain. Cost effective, F-Secure's Protection Service for Business (PSB) is a fully hosted automated solution - no management platform investment or maintenance is needed after installing the client software. In other words, you don't have to worry about managing upgrades, understanding virus definitions or installing in-house management servers.

By outsourcing you'll be able to provide the highest level of protection to your business, ensuring its ongoing IT health, and at the same time cutting costs and IT resource needs. An outsourced solution isn't just for the big-boys, even SMEs can benefit both practically and financially.

PSB is a complete protection service for desktops, laptops, file servers and exchange servers providing Anti Virus, Anti Spyware, Spam Control, Application Control, Firewall, intrusion prevention, Rootkit detection, Proactive 0-day protection through Deep Guard 2.0, a cloud-based reputation lookup service.

For more information please visit - www.f-secure.co.uk or call 0845 890 33 00



NEWS

STEP 4 BE PREPARED

Take a proactive approach to guarding against cyber threat

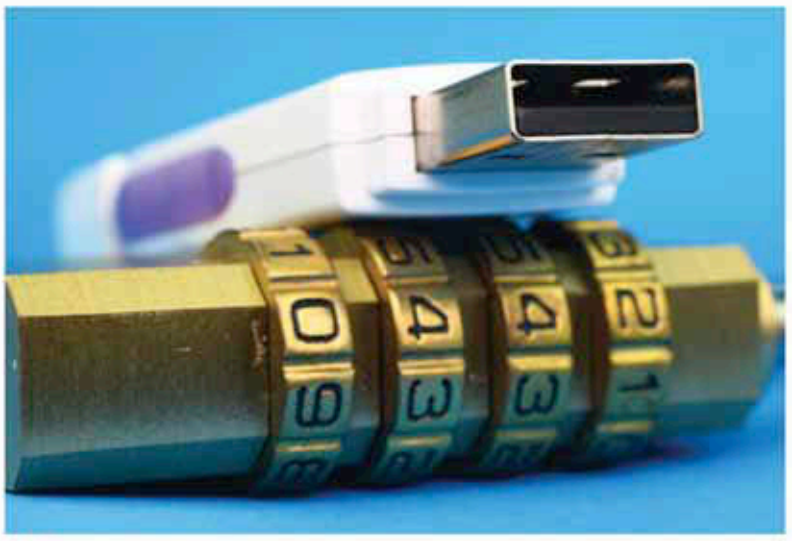
Question: New technology has brought with it new risk. How can a company guard against potential attack?

Answer: You can protect your business if you get the right advice.

We live in the information age, but as companies use increasingly sophisticated technology, so they open themselves up to potential fraud. And as the technology develops, the threat of attack intensifies. Whereas until recently, a company, Government or even individual, would become aware that something was wrong because, say, a website had been defaced, these days attackers are more data centric and stealthy, and it could be days before the victim realises it has been hacked into.

"When you talk to executives about cyber security, they think in terms of encryption, firewalls and IDSs," says Dr Eric Cole, a leading edge security consultant and fellow of the SANS Institute, which offers security training globally. "They need to understand the source of the vulnerability and implement automated, effective solutions. Organisations have to stop being reactive, you must be proactive."

And this is an issue that affects everyone who uses the internet, from an individual to a huge corporation. "At least 75 per cent of organisations have been targeted," says Dr Cole. "They must be properly protected or the chances of attackers getting in are extremely high. There have also been several cases of countries going after one another. Some industries are at particularly high risk, including the pharmaceuticals industry. They lose billions of dollars a year through stolen or knock-off drugs. Large manufacturers are also at high risk. Banks are targets, too, but they are often hard to get into, so an attacker is more likely to go after a medium sized merchant with data about credit cards. Wireless activity can provide a very easy entry into a network. Any company, especially a medium sized one will be a big target, as will hospitals and small health care providers, because they all hold PII - personally identifiable information." Once in possession of this, identity threat is a real risk: the fraudster will either use it or sell it on.



BE PROTECTED: By knowing what's out there we are more prepared PHOTO: ISTOCKPHOTO

The key to fighting this is to focus on threat and vulnerability. Threats come in the forms of worms, viruses and cyber hurricanes. Vulnerability comes through unpatched systems and extraneous surfaces. Most corporations are more focused on the threats, according to Dr Cole, which means they wait until an attack before they act. Most do not understand the speed at which potential fraudsters can now move: whereas until recently, it might have taken three to six months to break into a system, now it can take minutes, which means it is more crucial than ever to have the relevant software in place.

VIRGINIA BLACKBURN
virgina.blackburn@mediaplanet.com

FACTS

Credant Technologies suggests the following to ensure you keep your data safe on the move.

- Encrypt your data on every device you carry. As everyone now uses personal devices to link into the corporate network, be sure you can accommodate every type of file.
- Get a solution which can detect devices trying to connect to the enterprise and sync up with corporate data.
- Make sure your encryption solution does not slow your system.
- Never leave data security up to the end user. It is imperative that this is controlled and managed centrally. This can reduce costs as machines don't need to be locked down or bought into the office to update them.
- Corporate Governance requires you now to have security. Use a solution that includes a central management console – that way every machine can be tracked.

A step-by-step guide to eliminating risk

Many companies do not know where to begin to implement security procedures. The SANS Institute has created a thorough guide

One weapon in the fight against cyber crime is a document called the Twenty Critical Controls for Effective Cyber Defense, developed by the SANS Institute. "The idea it is that even though a lot of organisations have defences such as firewalls and encryptions, they were still being broken into, so they weren't doing the right things," says Dr Eric Cole. "These steps have been developed learning from the offense to build a better defence."

The system was set up to look at common vulnerabilities attackers use to break into organisations, and save companies money, had to be automated. "If you create a base line and automate it to run regular audits, you'll see better results," he says. "Organisations do an ok job of implementing security, but not maintaining it."

The controls starts with an overview of knowing the system through auditing, and takes into account hardware, operating systems and software. It tests perimeter controls: firewalls, IDSs, and makes them secure. It brings the system up-to-date, protects data and finishes with incident response and penetration testing. Visit www.sans.org/cag

YOU DON'T NEED SPY GADGETS TO TRACK YOUR COMPUTERS...

...YOU JUST NEED ABSOLUTE SOFTWARE

Organisations risk costly litigation and public relations nightmares when even one laptop goes missing – Computrace® One™ by Absolute® Software can help avoid that.

Absolute is a world leader in the security and management of mobile computers. Our patented firmware-based software enables computer theft recovery, data protection and IT asset management delivered on a subscription basis.

- Recover missing computers
- Post-theft forensics
- IT asset management – on or off the LAN
- Asset discovery
- Data protection with remote data delete
- Theft deterrence

www.absolute.com

AbsoluteSoftware

PERSONAL INSIGHT

STEP 5 DO YOUR RESEARCH

These days, corporations need individuals trained up to the highest standards to **maintain their security** and are employing specialists to bring their companies up to speed, training both employees and recommending the best types of software to **fend off attack.** Dr Eric Cole is the man leading the **fight against cyber crime.**

An expert who teaches the fine art of defence

Dr Eric Cole is one of the leading names within the field of information security: a teacher and consultant, as well as fellow of the SANS Institute, Dr. Cole has focused on perimeter defence, secure network design, vulnerability discovery, penetration testing, and intrusion detection systems, working with both corporations and governments. He has a master's degree in computer science from NYIT and a PhD from Pace University with a concentration in information security. Dr. Cole is the author of several books, including Hackers Beware, Hiding in Plain Site, Network Security Bible, and Insider Threat.

"My primary clients are pharmaceuticals, large manufacturers and financial companies," he says. "They are prime targets for attack."

Dr Cols believes that the best way for a company to guard itself is via a proactive approach, in which it finds its own vulnerabilities before an attacker can. This is focused on two areas: unpatched systems and extraneous surfaces, both of which can let attackers in.

"Operating systems are extremely complicated today," he says. "When new software comes out, there will be glitches or updates, and it needs patches as a way to fix these. However, when a vendor makes a patch public, this is akin to telling the world there is a weakness in their software, which means the attacker knows there is an easy way to get in the box. Again, the time it takes to do this has speeded up: until recently, three to six months was a typical time frame. Today, an attacker can take the patch and use it to reverse engineer into a system in less than a day, so companies need to proactively fix their patch as soon as it comes out."

The way an attacker typically attacks a systems is by finding visible IP's, identifying open ports and finding vulnerabilities in the services. There are a number of ways in which these vulnerabilities can be made more safe.

"A company should reduce the number of systems it has available from the internet," says Dr Cole. "Close down all the ports you don't need. You should also turn off unnecessary services: a lot of corporations have a lot of extra codes that aren't needed, and if you do that it is harder for people to get into a computer system."

INSIGHT

"When a vendor makes a patch public, this is akin to telling the world there is a weakness in their software."

Dr Eric Cole
A fellow of the SANS institute, Dr Cole is only too aware of how much is at stake

One of the biggest problems, of course, is that companies are either complacent, and don't believe they'll come under attack, or will have got away without proper security for a certain amount of time and thus feel disinclined to pay for the expertise and the software that will be needed to withstand attack. But the bigger the company, the more essential the security needed: a company such as a large online retailer, for example, is estimated to have 26 million credit card details on its database, and as such has to have a failsafe system in place.

But even smaller companies need to know the risk. A start-up, with, say, 50 employees, will probably have a lawyer and an accountant in place, but not someone in charge of security, and that encompasses not only IT, but human resources and every other aspect of company management as well. If someone is on board from the very beginning, conversant with developments in technology and understanding of the company's needs and risk of attack, it is guarding itself even before an attack can take place, the kind of training provided by Dr Cole. on the "Twenty Critical Controls for Effective Cyber Defence".

5 TIPS

Beat the criminals at their own game

1 Perform good asset management. Know what systems and services are running on your network. When organisations are broken into, the attackers find a vulnerability the company didn't even know it had.

2 Perform a policy of least privileged at every level of the organisation. Give every person the least access they need to do their job. If they only need email, only give them email.

3 Build an in-depth defense. Never rely on a single measure to protect your organisation. If it is compromised, attackers could bypass it. If you have many entities guarding you and one is bypassed, another takes over to protect your information.

4 Automate as much security as you can and audit it on a regular basis. Most organisations will go and run their scripts once or twice a year, but that allows a vulnerability to develop as the scripts deteriorate over time. If you want to fix a problem before it starts, then you should be running your programs once or twice a week.

5 Keep it simple. If you make guard measures too complex, people are not going to do them.

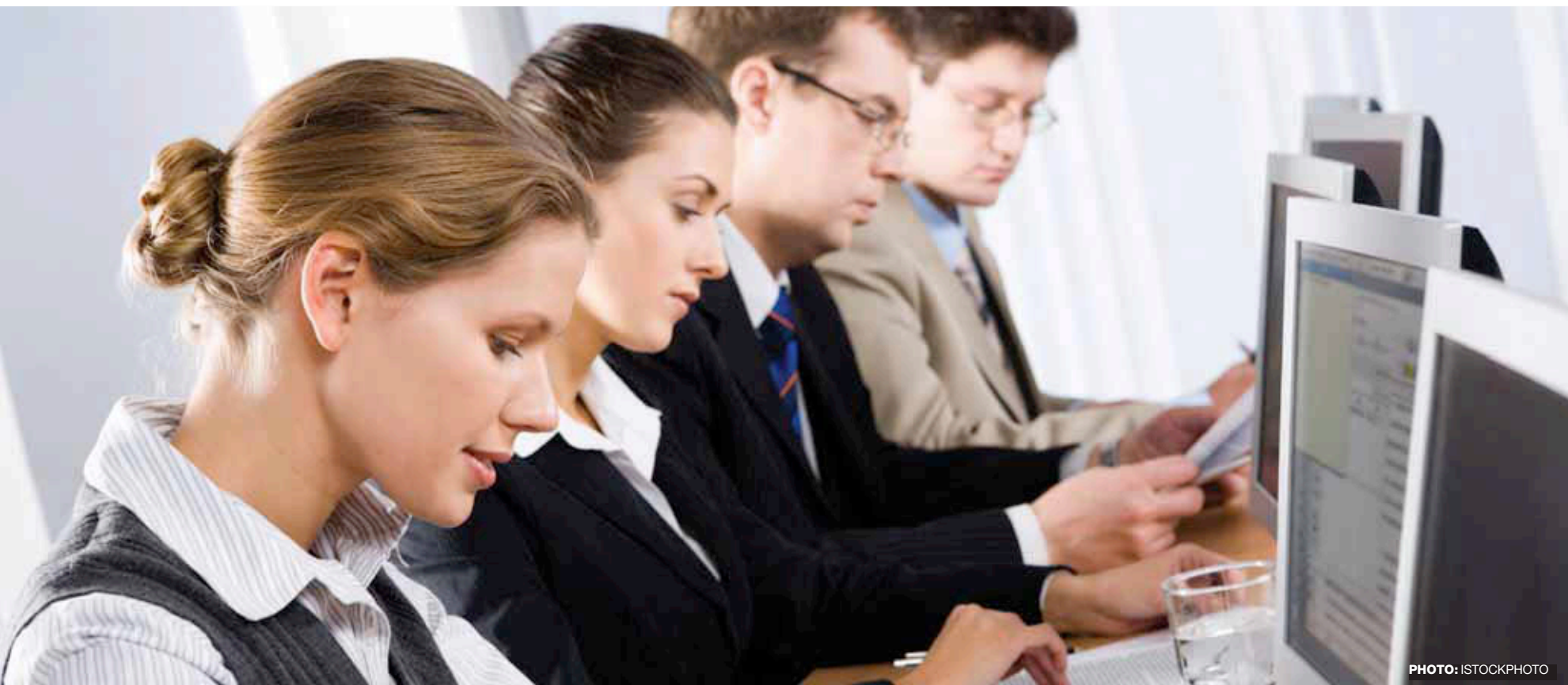


PHOTO: ISTOCKPHOTO

Web 2.0 – New threats need shared defences

Users are the weakest link

The boundary between home and work is blurring – workers take home corporate laptops or access work email and data through their mobile phones, while employers understand that allowing employees to perform some personal activities while at work keeps them motivated and in the office. There are now millions of people downloading music from the Web or visiting other recreational sites on their work desktops and with the potential for content and their personal information to spread virally; they're a scammer's dream. This year we have seen threats distributed via Twitter, Facebook and other social networking sites. Faced with the growing severity of these Web-based threats, as well as new threats that are appearing every few seconds, organisations should undertake a number of important defensive measures to protect their users, networks and data.

It is clear that organisations must look at ways to protect themselves from malicious content that can be delivered via downloads, however, they must also protect themselves from unmanaged employee use of applications such as unauthorised peer-to-peer file-sharing systems, consumer-oriented instant-messaging clients, consumer voice-over-IP applications and the like that can be the conduit for loss of sensitive corporate information.

Cybercrime is big business, and like any enterprising organisation, cybercriminals follow the money. As more people are drawn to the intensely collaborative and interactive nature of Web 2.0 for business and personal use, so too are the criminals. Web 2.0 technologies, such as Twitter, Facebook, LinkedIn & YouTube create a rich experience and open environment where everyone can contribute. But this opens more doors to security risk, by creating additional surface areas for attack and punching holes in traditional security boundaries.

Focus on the final link, not the initial problem

However the threat is initially delivered, there's a common weakness. "With Web 2.0, threats can hide anywhere, but the malware is always behind a web link. There's always a final URL that downloads the executable" says Mikko Valimaki, Chief Scientist at Blue Coat Systems.

Some vendors have released reports on the number of legitimate sites that have been infected, sometimes even blocking these sites though the real threat is elsewhere. It is important to reduce the problems of site infections, but blinding blocking anything that may unfortunately have been compromised has led to businesses going offline without necessarily stopping the real source of the threat; the final web page that these infections point to.

What can organisations do?

Companies should deploy a variety of tools in a multi-layered architecture to monitor, manage and control the use of a growing variety of applications that are used in the workplace. As threats are constantly changing, the system must also be able to provide instant reviews of new web pages so that a new threat is identified even for the first potential victim. A layered defence should be deployed that gathers together reputation, web text inspection, malware scanning and the sharing of threats from organisations that understand spam and those that understand web content. The ultimate goal is to keep users safe and advise them on threats to the organisation of data leakage while ensuring compliance with corporate, legal and other policies.

Employ a community based Web infrastructure

Deploying a neighbourhood watch-based approach has distinct advantages over conventional centralised web-spider crawling for bad pages. As we know; web pages can be infected at a moment's notice, so a daily crawl from a single vendor leaves web sites unprotected except at the instant that the crawler inspects the page. Phishing sites may be active for no more than a few minutes – the criminals can set up a page that looks like a bank and send out a million emails, as soon as a few customers have been caught, take down the site, empty the victim's accounts and repeat.

You can't defend against these threats alone. A large group of users can access tens or hundreds of millions of Web pages daily, providing a constant stream of fresh information about Web pages and therefore more readily detect new infections. As an example, Blue Coat's WebPulse cloud service gathers knowledge from more than 55 million users in large organisations, over 50 million users on ISP and mobile networks and around 1 million consumers – each user adds to the knowledge of the whole when surfing the web and WebPulse therefore receives over a billion requests and updates a week.

Shared defences are stronger defences

Organisations should ask their supplier how they gather further information and inspect pages for threats. Does the organisation cooperate with other vendors and use multiple technologies to inspect the web? As most email spam now contains a link to the real source of the threat on the web – email and web companies should be sharing their knowledge for the greater good. Online malware scanning and feeds from Google of known bad or questionable sites also increase defences from the single-vendor solutions. The key for such a defence is a significant volume of traffic analysed repeatedly by multiple anti-malware defence, machine analysis and human raters to provide reliable feedback on threats. Volume provides visibility and repetition provides timeliness across a large volume of web content which no one organisation can analyse.

Employ granular management and check the validity of old policies

It is clear that organisations need to enable certain web 2.0 applications to realise the productivity gains they offer for their employees. For example, LinkedIn is good to find business contacts. However, organisations need to continue to protect their users from the myriad threats. Granular policies can allow text and graphics content while blocking applications, deliver warnings and advice to users and allow the organisation to define policies in the grey-areas of the web where malware may reside. As an example, IT can implement policies that deny all executable downloads from sites that are currently unrated, stopping dead in their tracks malicious downloads from brand new threats. Even if a PC is compromised, defensive policies can deny the malware from communicating back to the home site.

Keep users safe both inside and outside the organisation

A lot of emphasis over the last decade has been on keeping users safe while inside the organisation's own network, but today with laptops and mobile devices, data and Internet access are often not completely under the organisation's control. Happily, vendors are now delivering the same type of defences for remote users – keeping data and systems safe even when employees surf from home using corporate devices. Some vendors, such as Blue Coat, are even delivering remote device defence free of charge to customers who buy their office-based systems. As someone who works remotely most of the time, I feel safer in the knowledge that technology is constantly being updated to defend me from the latest attacks. The key is to be able to monitor and control access to critical technologies while protecting users and networks from malware, everywhere.

Nigel Hawthorn, VP EMEA Marketing, Blue Coat Systems • Nigel.hawthorn@bluecoat.com • www.bluecoat.com

SYMANTEC IS

No company on earth has a larger infrastructure solely for the purpose of tracking, identifying, and eliminating threats before they attack. At Symantec, we take cybersecurity very seriously. That's why we work 24/7 to protect your systems. Learn why 99% of the Fortune 500® depend on Symantec for their security.

SECURITY.

symantec.co.uk/dlp

Confidence in a connected world. symantec™