CYBERSECURITY

FINANCIAL TIMES **SPECIAL REPORT** | Thursday June 2 2011

God of gods
Joseph Menn explains why Zeus has been such a devil
Page 4

www.ft.com/cybersecurity-2011 | twitter.com/ftreports

Threats pile up in war that never ends

Intrusions are the norm while social networking and mobile devices are adding to worries, says **Joseph Menn**

Dark deeds: 'With the end-point security that average consumers get, they don't have a prayer', according to a security company president Alamy

For more than a decade, the task of securing a personal computer, corporate network or internet transmission from hackers has been one the vast majority of people, from chief executives and government leaders to consumers, have tried to foist on others.

That is understandable: the job is complicated, unproductive, and never finished.

But a series of shocking events in the past year and a half – from the Chinese electronic break-in at Google, to the Stuxnet worm's stealthy attack on the Iranian nuclear programme, to mass breaches of consumer information at Sony and elsewhere – have forced a broad recognition that despite the hardships, all those using the net must accept cybersecurity as part of their mission.

Chief executives, mindful of the brand damage that a Sony incident could bring and the potential for devastating industrial espionage, are now more likely than ever before to grapple with security issues themselves, according to surveys of their lieutenants.

Cyber intrusions are fast becoming the norm at the world's most sophisticated companies, including some that have security as their main mission.

A problem this year at RSA, the security company owned by EMC, a data storage outfit, prompted the US National Security Agency to warn that RSA's 40m physical tokens with fast-changing numeric passwords should no longer be sufficient to grant access to critical infrastructure.

The breaches are also reaching wider and lower, and not just through one-time assaults on the likes of Sony, which revealed details on 100m users of its online gaming networks.

Consumers' computers are increasingly at risk directly from virus infections that are undetected by standard security software and that do more harm than their predecessors.

The fastest growing type of infections install software that records keystrokes, including financial logins and passwords, and whisk that data off to overseas gangs that specialise in defrauding banks or taking over e-mail and social networking accounts to spread more malicious software, known as malware.

"With the end-point security that the average consumer gets, as well as small and medium businesses, they don't have a prayer", says Art Coviello, RSA's president.

Compounding and uniting the threats are two fast growing phenomena.

The first is social networking, in which individuals give all sorts of clues that can be used against them in phishing scams.

Those services have also trained users to click on shortened web links that could lead to malicious pages.

Targeted e-mails to employees, made more credible by public information about the recipients, are the delivery method of choice for intrusions such as those at Google and RSA.

The second is the rise of mobile devices, which are generally controlled by employees but often have workplace access and are just beginning to be targeted in earnest.

> 'You sometimes have perverse incentives that encourage underinvestment in security'

The core problem is the combination of the most open and interoperable network ever designed and the rapid development of more powerful software and devices that take advantage of it.

It is in large part a blessing, of course, and one that is responsible for $10,000bn in annual transactions.

But various criminal groups, some linked to traditional organised crime, national governments, or both, are taking advantage as well.

They are excellent capitalists, making money from one scam and reinvesting in new research and development to stay ahead of the security profession.

"For every technological or commercial quantum leap, criminals and criminal syndicates have kept pace," commented Eric Holder, the US attorney-general, this month.

He added: "Cybercrime threatens the security of our systems as well as the integrity of our markets."

The advances in software and the increasing use of the internet have made defence more difficult, not easier.

"Our defences are in many cases interlinked, and if one of them has a flaw that is all that is necessary for an attacker to get in," says Eugene Spafford, a security expert from Purdue University, Indiana, who most recently testified to Congress on the Sony breach.

He adds: "We have problems of scale and complexity to deal with, we have problems of time, of finance, of awareness. We have a lot of things going against us."

The lack of rules that has in large part spurred the growth of internet businesses has left no safety net in security.

Businesses are confronted with a dizzying array of solutions from speciality vendors who offer everything from standard firewalls to cutting-edge "behavioural analysis" that tracks when machines are connecting to new sites or at odd times.

Few offer anything comprehensive, and none guarantees that hackers will not find a way in.

Even worse than the fact that companies do not know what to buy is that they often do not want to try.

"You sometimes have perverse incentives that encourage underinvestment in security," Mr Spafford says."Sometimes people are evaluated on how much they save in spending, so they try to play the odds: `We didn't get broken into this year, so we'll postpone the upgrade until next year.'"

New regulations could well bring fresh problems, especially if bureaucrats require companies to install programs that combat the last wave of crime instead of the next one.

But the increased awareness of hacking has finally prompted government officials who eschewed regulation to admit that the free market is not doing the job and to take a more active approach.

In the US, the White House put forward a detailed set of proposed laws in May that would help protect critical infrastructure from Stuxnet-like attacks, using analysis based on the biggest risks.

The laws would also require more notifications of breaches and aid private industry more. Days later, the White House pledged to work more closely with other countries to improve their defences and take action against countries harbouring criminals.

The legislative package has a long way to go to get through a divided Congress, but lawmakers in both Republican and Democratic parties agree that more has to be done, and soon.

"Everyone who has a computer or a mobile device that connects to the internet is only going to come under more attacks," says Harry Raduege, a former head of US military information security who is speaking at the EastWest Institute's cybersecurity policy summit in London this week.

"What is lagging behind in all of this is the policy, the strategy and the approach that government and private industry need to take."

Inside

Spying The web has made it easier to launch attacks, as shown by the assault on Sony's PlayStation Network **Page 2**

Interview Data are the prime concern of Paul Wood, Aviva's chief security officer **Page 2**

Market chaos Options are overwhelming for small businesses and takeovers are not helping much **Page 2**

Social networks Tricking data out of people is not new, but the rise of Twitter has made it easier **Page 3**

Consumerisation Staff gadgets can imperil security **Page 3**

Malware economy Criminals rival Silicon Valley in development of business models **Page 4**

Country profile The UK has a three-pronged plan to thwart threats of cybercrime **Page 4**

More on FT.Com
Nick Chaffey of PA Consulting Group says many companies are playing cyber roulette with their business, and do not even know the odds.

Battle is joined on two fronts

Vulnerabilities

'Hacktivists' add to the threat posed by sophisticated criminals, writes **Stephen Pritchard**

The idea of the computer as something that could be attacked, let alone something that could be used to attack others, was simply not a consideration in the early days of personal computing.

As a result, the IT industry has been playing catch-up with hackers and cybercriminals for decades. "The bad people in cyberspace will not go away, and vulnerabilities will not go away," said Steve Ballmer, Microsoft's chief executive, in 2004.

The vulnerabilities have indeed not gone away. In many respects, despite the best efforts of Microsoft and others, they have become significantly worse.

The situation is further exacerbated by growing evidence of politically motivated attacks, and in some cases government-backed attacks over the internet, targeting organisations and companies that use it.

The Anonymous group's attacks on several high-profile companies that had severed their commercial links with WikiLeaks, following that site's release of US diplomatic cables, illustrates that there is more to the cybersecurity threat than the work of criminal gangs.

Malcolm Marshall, head of information security at KPMG, warns: "Hacktivists don't operate on a profit and loss basis but are ideologically motivated and have significant resources behind them. The emergence of electronic espionage and especially hacktivism has shifted the ground in the corporate security landscape."

One result of that shift is that tools and techniques that deter criminals might not work on other groups. If a business increases the cost to a criminal of breaking into its networks, through better security, the criminal is likely to look elsewhere for a less challenging target.

Marshall: ground has shifted

But hacktivists are less easily deterred. Large, co-ordinated attacks using relatively unsophisticated malicious software, or malware, have brought down systems belonging to companies including Visa and PayPal.

Groups are even using their size and scale to revive obsolete malware, opening up vulnerabilities that many in the industry believed had been blocked.

"Eighty per cent of the vulnerabilities we are seeing, we've seen for years," says Mike Maddison, partner in security and privacy services at Deloitte.

The result is that businesses are forced to defend themselves on two fronts: against highly skilled cybercriminals, using new tools and exploiting new security loopholes; and against less sophisticated attacks that rely on sheer weight of numbers.

Continued on Page 3

Gatekeeper at Aviva rises to the threats

Interview
Paul Wood

Data are a prime concern of the chief security officer, says **Jessica Twentyman**

From terrorists to shoplifters to computer hackers, Paul Wood, group chief security officer at Aviva, the UK-based insurance group, has the professional experience to handle almost any threat he encounters.

He spent 21 years as a counter-intelligence officer in the military police, followed by a short stint running a convenience store in Taunton, Somerset.

He worked in security jobs at the Civil Aviation Authority, at an internet security specialist, and at UBS, the financial services group, before joining Aviva in May 2006.

Today, he is responsible for all aspects of security at Aviva, but information security is the one that takes up most of his time, probably as much as 80 per cent, he says.

When he joined Aviva, the business was still very federated and there were only two people dedicated to information security at the global headquarters in London.

Now, there are close to 20. Growing and developing that team has been an important focus for Mr Wood over the past five years, he says.

Alongside that effort, he has also overseen a wide variety of information security projects around systems and network access. These include refreshing the company's security technology infrastructure and establishing consistent approaches to tackling malware and supporting remote access for employees in the field and at regional offices.

At the same time, he faces the constant requirement to monitor the threat landscape and analyse how new and emerging threats might pose a risk to Aviva.

This involves sifting through reports and alerts as soon as they are published, working with vendors with specialist skills and networking with information security professionals from other companies.

"It's really important to hear about issues that others have faced, and to learn from their mistakes. This provides me with valuable clues as to where potential areas of exposure lie in my own company and enables me to shut them down quickly," he says.

"These interactions are what enable a security chief to work out what threats particularly bother you or might keep you awake at night, and ensure you have sufficient focus on and understanding of how you're going to tackle them to enable you to sleep soundly," he says.

A top-level security role such as Mr Wood's inherently calls for an unflappable personality that can deal effectively with ambiguity and "unknown unknowns" in a businesslike way. Mr Wood has that.

"There's not ever going to be no risk to a business," he reasons.

"Sometimes, the security industry overhypes the risks that are out there. One thing I've been pretty firm about in my approach to the job is that you simply can't use media hype to argue a budget out of the organisation. You have to be able to demonstrate that a particular risk is real."

Practical help and day-to-day support, meanwhile, is on hand in the form of an executive team that comprises five regional chief information security officers. "They're out there finding their own issues and concerns and bringing them back to me, so that we can all work together on defining how they should be addressed in a globally consistent way."

Mr Wood reports to Cathryn Riley, Aviva's group chief information officer, who in turn reports directly to Andrew Moss, the chief executive, and sits on the group executive committee.

Mr Wood is regularly invited to brief the committee. In recent weeks he has talked to them about current terrorism risks and the implications of the London 2012 Olympic Games for Aviva, and security standards at the company's London headquarters.

At the same time, he is working with the IT architecture team to define new security profiles for various pieces of infrastructure and managing a project review of a continuing implementation of software from Sailpoint, the identity management specialist.

Looking ahead, there is Aviva's Microsoft Active Directory structure to review, an intrusion detection system to configure, and a mooted project to establish a global security operations centre in North America with Symantec, the IT security company, to explore.

With all that on his plate, it is perhaps fortunate that Mr Wood is able to sleep so soundly at night.

Paul Wood: regularly invited to brief Aviva's group executive committee

Spying rife as web adds to risks

Industrial espionage

The internet has made the task of snoopers easier, says **Maija Palmer**

With a multibillion-dollar research and development budget and a leading position in the computer chip sector, Intel has been the target of constant industrial espionage efforts. However, methods have evolved over the years.

In 1993, when an employee tried to steal designs for a microchip, he did so by videotaping data on his computer screen and posting it to rival company AMD. Five years later, another employee copied design details from the network on to his laptop.

In late 2009, Intel is thought to have been one of more than 30 companies targeted over the internet by Chinese hackers.

In fact, industrial espionage has become such a persistent problem for Intel that in 2010 it became one of the first companies formally to include this as a risk in a statutory report to the US Securities and Exchange Commission.

But Intel is far from being alone. Computer security professionals believe that most companies are at risk of some kind of attack.

A report by the UK cabinet office this year estimated that cyber espionage was costing the UK economy some £17bn ($27bn) a year. German counter-intelligence experts have maintained the German economy is losing about €53bn ($75bn) or the equivalent of 30,000 jobs to economic espionage yearly.

"This sort of thing is happening much more often than most company boards believe," says Henry Harrison, technical director at Detica, the information security company.

Mickey Boodaei, chief executive of Trusteer, a security company, says: "The numbers are hard to quantify. For every attack that becomes public – such as RSA or Sony – there are hundreds, if not thousands of smaller attacks that are not reported.

"Most are under the radar and might not be discovered for days, or weeks – or even years."

Companies are often reluctant to report attacks, for fear their reputations will suffer.

When a company loses customers' personal information – such as in the case of Sony's PlayStation Network – they are under obligation in many US states to notify the clients. As a result, breaches often become publicly known.

But there is no obligation to go public if a product blueprint, a marketing strategy or some other commercially sensitive document has been stolen.

Security professionals all have stories about cases when a company has refused even to report an incident to the police.

While industrial espionage has always existed in the commercial world, IT experts say the problem has become much worse recently, because it is relatively easy and risk-free to attack companies through the internet.

"Historically, there was always some element of personal risk in industrial espionage – you had to go physically into the building and remove documents. But now you can do it from the other side of the world with very little chance of prosecution," Mr Harrison says.

"Espionage has been going on for ever, but the volume of it is so much higher, that is what people are now trying to get their heads round," he says.

This month George Osborne, UK chancellor, disclosed that the UK Treasury was being bombarded with about 20,000 malicious e-mails a day, giving some indication of the volumes that businesses may be having to deal with.

You do not have to be an IT genius to be an industrial spy. Mr Boodaei says it could take only about 10 hours for a moderately computer-savvy person to put together a program to penetrate a corporate computer system. Information on software flaws that can be used to get through to a corporate network is freely traded on internet chat rooms. "It is similar to learning how to make a bomb on the internet. With basic skills, you can build something like that quickly," Mr Boodaei says. Attacks are hard to detect.

The rogue software is designed to be unobtrusive in the company's computer system.

"If you see a computer behaving strangely, slowing down or having trouble connecting to the internet, it is a sign that it is infected with something quite unsophisticated. Most attacks now are much more sophisticated," Mr Boodaei says.

The trail of who has stolen the information is even harder to trace.

When Google was hacked in late 2009, it pointed the finger at the Chinese government, prompting a partial pull-out of operations from the country.

In 2007, Jonathan Evans, head of the UK's MI5 security service, sent out confidential letters to 300 chief executives and security chiefs at the nation's banks, accountants and legal firms warning them of attacks from Chinese "state organisations". Security experts also say that many attacks originate from Russia.

But it is hard to be precise about their origin. Any moderately skilled hacker will be able to route the attack so it appears to be coming from some completely unrelated business and country.

The attack may appear to come from a small real estate company in California, or the offices of a Chinese newspaper, while these businesses are completely unaware their computers are being used.

This is why many companies – and their security advisers – do not bother to trace the attackers; they just focus on stopping them.

"When the chief executive is informed, his objective is almost always just to try to get the intruders out of the system. Suppose you did track them down – what are you going to do? Put the international law enforcement system to the test?" Mr Harrison says.

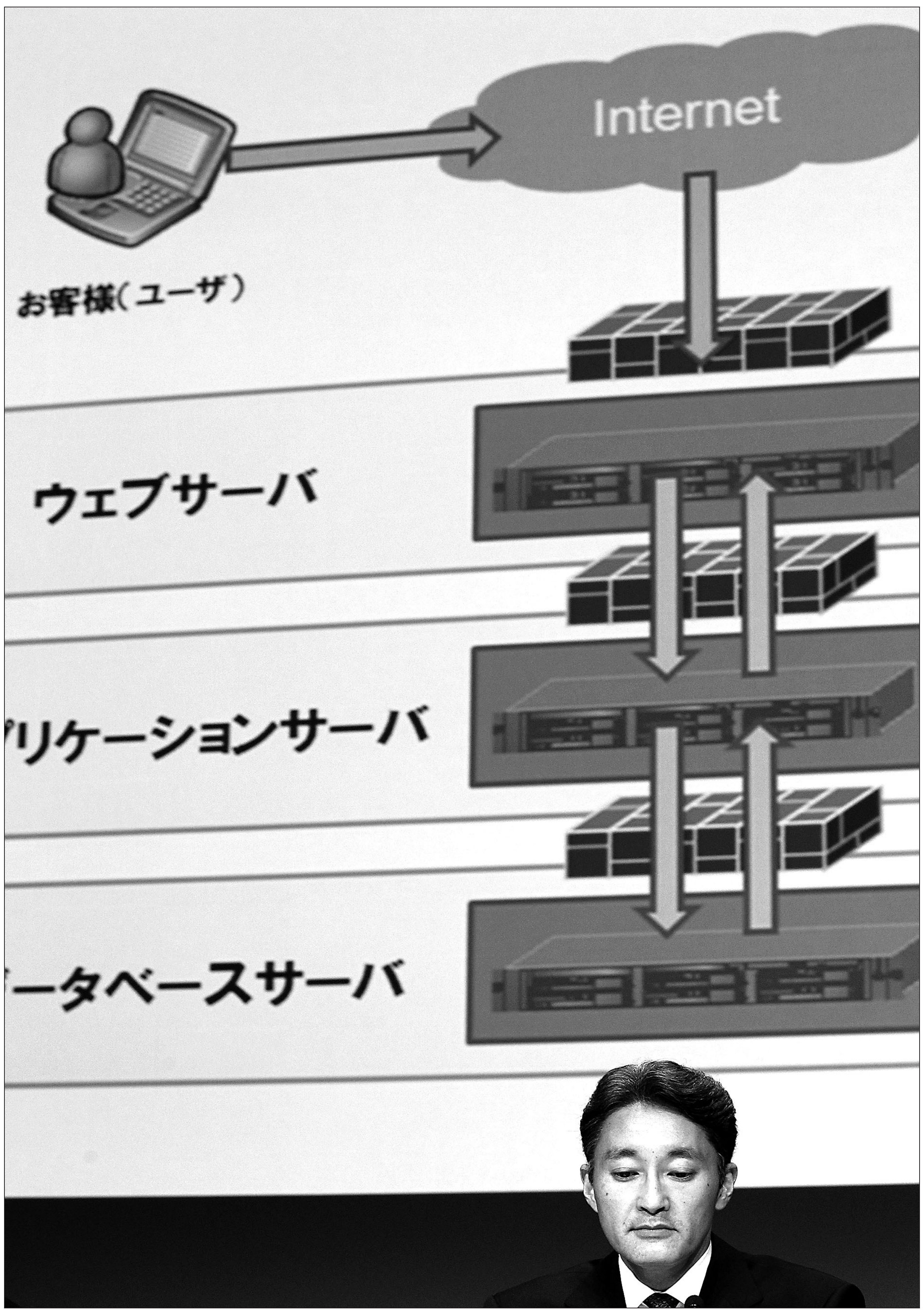
The good news is that there are plenty of security companies offering ways to protect corporate information. These often involve monitoring for suspicious behaviour on networks and keeping track of who is accessing important documents. It is like installing an electronic CCTV camera on the network.

Security does not have to be about buying a lot of expensive equipment. "I get frustrated by companies that spend a lot of money on security software but won't consider the simple stuff," says John Walker, a member of the ISACA security advisory group.

He recommends starting with simple measures, such as identifying important information that needs protecting and thinking carefully about different ways intruders could get in.

"Companies should look at something as simple as a printer. New printers have enormous hard drives and are often connected to the internet. But often no one has thought of that as a security risk."

The trail of who has stolen the information is even harder to trace



Kazuo Hirai, Sony Corp executive deputy president, reveals PlayStation Network hacking data Reuters

Safety first Ten tips for companies to improve cybersecurity

● Elevate cybersecurity issues to the chief executive. Security should not be treated as a subset of information technology or similar responsibilities. Budget considerations require a fresh approach: the benefits are less tangible than the costs yet can prevent catastrophic losses.

● Conduct regular security audits. At least once a year, bring in professionals to identify the most easily targeted parts of your operation, the most likely methods for attack, and the strength of your existing defences. A thorough audit should include penetration testing, where professional hackers try to break in.

● Assume that if you have not been hacked, you will be. Invest in software to monitor all network traffic and especially track outbound connections. Hackers not only have to get in, they have to get the data out again.

● Identify your most critical digitised assets and isolate them. If at all possible remove them from networked machines. Develop a strict procedure for access. For other data, grant access only to employees who need them.

● Acknowledge the death of the "perimeter defence". Employees will bring in portable miniature drives that connect directly to networked machines, and some of the drives are likely to be infected. You need a layered defence that works on multiple levels simultaneously.

● Use active gateway protection. One of the easiest means of entry into a company is through a website with malicious content. Security programs that block websites with poor reputations are not enough, because some attacks are staged from legitimate websites that have been induced to serve trick advertisements. A better bet is defence software that checks every page visited for bad code.

● Exercise caution with mobile and other remote access. It is always easier to compromise a consumer's machine than a workplace machine. Either assume full responsibility for securing all employee devices that can access company assets or set strict limits on what those machines can do.

● Train your workforce – all of it. E-mails to senior executives that appear to come from colleagues or customers, referencing relevant material, may be laden with programs that provide back doors for hackers. But the rank and file must be educated, too – wherever they go on the internet and whatever software they use could expose the company.

● Patch your systems. A great number of hacking incidents can be avoided with the timely installation of patches that have been issued by software makers that are aware of vulnerabilities.

● Minimise the amount of power that employee machines have and the data they retain. Do not give out administrator ability to install new programs easily, and closely monitor those who have it. Reduce the data kept about customers to what is really needed, encrypt it, and delete it when there is no good reason for keeping it.

Joseph Menn

Market chaos leaves small businesses as primary target

Consolidation

April Dembosky finds SMEs overwhelmed by choice – and vendor takeovers are little help

The Lincoln Racquet Club in Lincoln, Nebraska, would not consider itself the prime target for cybercrime. It hosts racquetball tournaments and offers fitness buffs the latest exercise bikes.

But those bikes are linked to the internet where riders record the miles they have cycled, and the racquetballers access an open wireless network to change tournament rankings online. Both link directly to the club's database, where details of about 1,500 credit cards are stored.

The club's first line of defence is Della Johns, general manager and what people in the computer industry call the "accidental IT guy" – or gal, in this case. She spends most of her time scheduling aerobics classes and hiring personal trainers.

But because Ms Johns also knows how to edit the website and set up an e-mail account, she has become the de facto IT expert. That means she is in charge of coming up with a cyber defence system, even though she does not know the difference between a worm and a botnet.

"I know we need protection, but I don't know what the best thing out there is," Ms Johns says.

The fact that there are thousands of security products on the market designed to help businesses such as the Lincoln Racquet Club merely creates another problem for Ms Johns, rather than a solution. She has no time to research firewalls or price antivirus software.

"Small and medium sized business are completely overwhelmed by the options," says Tebrez Syed, vice-president of products at Spiceworks, an online network of IT professionals.

That is the main reason small businesses have indeed become the primary target of cybercriminals, says John Pescatore, Gartner security analyst, precisely because they are so lost when it comes to security. Hackers would much rather prey on several small businesses that inadvertently leave the back door to their network open than one large bank where they have to drill through the cyber equivalent of a concrete safe.

Big companies such as Dell and Hewlett-Packard say they are on track to fix Ms Johns' problem. Both have made a series of acquisitions of security companies in the past year that they say will help consolidate the market for the better.

Dell bought SecureWorks. HP bought ArcSight and Fortify. And while these companies' technologies are quite advanced, the acquirers say the concentration of knowledge will soon trickle down to small businesses as far flung as Nebraska.

"For a long time, computer vendors have been like car makers that make cars with no brakes, no air bags, no seat belts," says Chris Whitener, HP's chief security strategist.

"What we want to do is make sure security is baked in to everything we do. If you get a router, it's got security in it. If you get a laptop or a printer or a server, you have all the elements you need."

But analysts are sceptical of the strategy.

"When an infrastructure company such as Dell, HP, Cisco, or IBM buys a security company, they usually screw it up," says Mr Pescatore.

"Everyone who manages computers knows you can't trust the infrastructure to protect the infrastructure."

Start-ups respond to new threats, grow up, get acquired and the cycle repeats, says John Pescatore

For every company that gets acquired, he says, several more start-ups develop to take its place.

"We're in this period right now where the threats have got ahead of the protections," Mr Pescatore says, referencing the recent breach at Sony that exposed account information of 100m people. "Whenever that happens is when we see these bursts of start-ups that are quick to address the new threats. Many grow up, get acquired, and the cycle repeats."

Mr Tebrez at Spiceworks says social networks such as his, where bona fide IT people have reviewed 20,000 products, are the real key to helping small businesses navigate the market.

"I'm seeing the democratisation of information," he says. "In the past, information was controlled: who placed magazine ads, who made announcements, who did a dog and pony show in front of analysts. The shift that's taking place is people can talk to each other. They're telling you the real deal."

Justin Davison is a senior systems engineer for the RJ Lee Group, a chemistry lab near Pittsburgh, Pennsylvania. He says he prefers to ask his colleagues in the industry for recommendations.

"I don't completely trust a vendor to look out for my best interests," he says. "Whereas my peers have no ulterior motive, they don't make a commission."

It is these peer-to-peer recommendations that Ms Johns has come to rely on, albeit indirectly, to secure the member information of her racquet club.

She ultimately hired a consultant, one who uses the Spiceworks network, to separate public and private networks and choose the best malware scanners and vulnerability management software.

"You're at the mercy of the technical people," she says, "and you just hope they know what they're doing."

Employees' devices present problems for corporations

Consumerisation

Security can be compromised by staff gadgets, says **Chris Nuttall**

First it was sexier laptops appearing on desks, then smartphones, now tablets. A "consumerisation of IT" trend has brought whole new categories of devices into the workplace that are voluptuous to the eye but vulnerable for the network.

The appeal of the BlackBerry and the desktop PC is waning and workers are finding their own chosen devices are powerful enough to handle personal and business needs. With the most senior management wanting to use their Android smartphones and latest tablets for work purposes, IT departments can lack the ability to implement effective security policies.

"It's not just the C suite who are bringing their devices in and expecting to get them hooked up, and it's not just one single function such as the sales department," says Jamie Barnett, senior director of mobility product marketing for McAfee, the US security software company.

"In many cases, it's everybody, and I think companies are also realising it's a cost-saving opportunity for them."

Research commissioned by Dimension Data suggests half of UK businesses permit the use of employee-owned devices and 39 per cent of those doing so are not using encryption to protect their corporate data.

About one in five companies also allow staff to access the corporate network remotely using their personal gadgets, without insisting that antivirus software is installed.

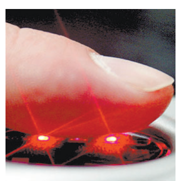
The lack of protection means accidental data loss by employees is a growing problem. Their trendy smartphones, tablets and laptops also have that extra appeal that makes them prime targets for thieves.

Thieves can also steal more than the hardware, with smartphones often containing more useful data than a laptop.

"They can get access to really important personal details that can help with the social engineering attacks we are seeing," says Mr Barnett.

"If you get access to my mobile device, you can see who my contacts are, who my kids are, so that if you were a savvy cyber criminal you could "spear-phish" me and make me a very attractive access point to critical business data."

Device makers are beginning to introduce their own security features in these consumer devices – Apple's Find My iPad/iPhone will locate a missing device on a map, remotely lock it, and even erase all data on it. But there is still no common approach.



Fingerprint recognition may be installed in mobile devices to secure them better, says Unisys

"Control and consistency are the two main things you miss out on when you allow workers to bring in their own equipment," says Neil Campbell, global general manager of Dimension Data's security business.

"You have no direct control over the device, the version of the operating system, whether they have antivirus, firewalls or encryption software, so organisations don't know about functionality or risk."

Technology to deal with vulnerabilities is also running behind, as is the implementation of what is available to deal with threats, he adds.

To cite one example from McAfee's quarterly threats report: Google had created a security repair tool for virus infections on Android devices that malware creators faked as the official Android Market Security Tool. Their version monitored incoming SMS messages and was able to steal data and phone information from those who had installed the app.

One answer to the problems may be a device that is both appealing in looks from a consumer point of view and secure from a corporate standpoint.

Enter Google's Chromebook, available from Samsung and Acer this month in the shape of a slim, instant-on laptop with long battery life and minimal data storage due to all the user's information being accessed through an internet browser and stored in the cloud.

Such was the corporate interest that 50,000 businesses asked to try out the prototypes when they were unveiled and Google is hoping to switch over most of its staff to using Chromebooks over the next year. "It really simplifies our job from an IT point of view – just the management of all these things," Sergey Brin, Google co-founder, said at a launch event.

"It really improves security . . . you lose security when you add complexity; it's any extra thing you need to install or can install, any driver, all those things add attack services, so we're going to be deploying them increasingly internally."

Unisys, an IT group, sees companies taking a number of steps to meet the new challenges. It predicts companies will start changing policies to ensure authentication of the identities of device users and encryption of enterprise data across the network.

Biometrics – iris, fingerprint, facial or voice recognition – will be introduced in mobile devices to secure them better, it forecasts, and location-based technologies such as GPS will be used to limit employees' access to data according to where they are – for example, restricting access to sensitive information in public places.

That may sound Big Brother-ish, but it is the price employees may have to pay in exchange for the freedom of choosing to use their favourite gadget for both work and pleasure.

Crooks cash in on the need to chat

Rotten apples: Tweets that mention iPad or iPhone have prompted spam-style replies enticing people to click on a shortened link Alamy

Social networks

Tricking data out of people is not new but is now easier, says **Tim Bradshaw**

Facebook, the 600m-strong social network, has a mission: it wants to connect the world.

Unfortunately, however, cybercriminals have quickly understood that the huge number of connections, viral applications and open sharing of information on platforms such as Facebook, Twitter and LinkedIn can be used for ill as well as good.

One notable example of the potential threat was when Sir John Sawers, shortly before he became the head of MI6, was alerted that his wife's ordinary use of Facebook could have put his family's security at risk by posting details of their children and house location.

The ease and comfort with which many of today's internet users post huge amounts of information about themselves online is a potential vulnerability that is only going to grow as younger generations enter the workforce.

"Since the premise of social networking sites is to share personal information more easily and efficiently, users tend to lower their guard," says Alastair MacWillson, global managing director of Accenture's security practice.

Many of the criminals' social-media tactics have been honed in other digital spheres, such as e-mail. Websense, an IT security firm, recently warned of a Twitter scam that attempted to lure unwitting users to a phishing site which aimed to capture their login details. "OMG CNN confirmed they found Osama alive still!!" read one of hundreds of tweets that Websense claimed were being posted every second, playing on the fascination around the killing of Osama bin Laden, the al-Qaeda leader whose death prompted more people to tweet over a period of several hours than ever before.

Accompanying the scammy tweet was a link cut down to a 140-character-friendly length using Bit.ly, the web-address shortening service. Bit.ly, along with its competitors such as TinyURL, abbreviates links in such a way that it is hard to discern the destination, making it even harder to tell truth from scam.

Because it is an open network, in which anybody can direct a public message to anybody else, Twitter has also become vulnerable to spam. Apple fans, for instance, may have noticed that whenever they mention iPad or iPhone, they have received replies from strange users enticing them to click another shortened link.

Whole networks of rogue Twitter accounts now exist to "retweet" these spam-style messages, so as to fool Twitter's anti-spam service into thinking that they are genuine. (*see http://blogs.ft.com/fttechhub/2011/03/twitter-spam/*).

For businesses, these could provide a route into the network for viruses lurking on the destination sites. But the bigger security risk posed by social networks is social engineering: the art of gathering information about specific individuals in order to fool them into giving away sensitive corporate details.

"Social engineering has always been easy because people want to use technology, but do not understand its complexities," says Alex Richards, a cybersecurity expert at PA Consulting. "Masquerading has become increasingly advanced because of the tools available via social engineering sites, and criminals have become more sophisticated. Despite this, the basics haven't changed. Impersonating someone else to trick people into giving information is not a new crime – it has just got easier in cyberspace."

> 'Not only are people being targeted but, inevitably, some of those attacks are going to get in'

George Osborne, the UK chancellor (finance minister), highlighted the risk of such attacks in May when he told a conference that the Treasury was hit with an average of one "serious and preplanned" attack every day (*see http://www.ft.com/cms/s/0/bf2dbc8c-7f9f-11e0-b9b0-00144feabdc0.html#axzz1NCyruOHj*).

The example he gave was an e-mail, identical to one sent around the department minutes earlier, but this time containing a malicious attachment.

Such a good spoof was an example of "spear phishing" – a precise attack targeted at a small number of people, often with the e-mail address appearing to come from a colleague or a friend.

"We're determined to get the security question right, so that we can maximise the opportunities that the internet age offers," Mr Osborne said.

Striking that balance is a familiar challenge to any corporate IT department. Yet companies are not approaching this new risk in a uniform way. A survey of 500 chief information officers commissioned by Hewlett-Packard found that half were planning to restrict use of social networking sites by employees – the implication being that half are happy to tolerate the risks for other reasons.

"I think the biggest risk to most corporates is people spending too much time on these sites and not doing their job," says James Alexander, a partner at Deloitte. "On services such as instant messaging, there is a potential for data leakage, but the biggest risk is reputational, both for the organisation and the people who work for it."

For Mr Alexander, the threats posed by social media are part of the broader trend of "consumerisation" of corporate technology. Companies that block Facebook and other sites risk outcry among their employees, who will in any case be able to access them from their home PCs.

"Privacy issues also exist around the employee-employer relationship," says Piers Wilson of PwC's information security unit.

Perhaps it is these concerns, not ignorance of the threat, that explains why just 17 per cent of HP's surveyed chief information officers are "strongly considering" putting in social-media security policies.

Many security experts advise education of employees rather than banning use of networking sites altogether. This, coupled with a good detection system to ensure that when someone does click on an infected link on Facebook or Twitter, the organisation can react quickly to contain the threat.

"We are asking our customers to get their heads round the fact that not only are they being targeted but, inevitably, that some of those attacks are going to get in," says Henry Harrison, technical director for cybersecurity at Detica, the BAE-owned firm.

"First, you accept that it is going to happen. Look for behaviours and things that are going on inside your IT system that look suspicious. Then go and investigate them."

Battle has to be fought on two fronts

Continued from Page 1

This is prompting security experts to look again at the basics of how organisations operate online, and how to protect those operations.

Applications were frequently designed on the basis that anyone who could access them would be inside the organisation's perimeter and so, was a legitimate user. Now, security experts say, it is necessary to assume that the perimeter will be breached.

So restricting access to applications, and encrypting databases, are among steps that businesses are taking. Advanced network and application monitoring tools also serve to alert security officers if there is a breach.

It is important, also, to see a business system as a whole, rather than as a collection of individual components, that is, to see it as a hacker would see it.

"Rather than looking at whether an individual technology or individual people are vulnerable, look at it as a coherent business system," advises Rupert Chapman, head of IT infrastructure consulting at PA Consulting. "You might be secure in one part, but not be securing the total."

Nor is it just older malware that poses a threat. It is also older security failings in applications, and the way individuals use technology.

Security experts warn that companies are failing to learn the lessons from the early days of laptop computing. Just as in those days, machines were often issued to staff without security software, so are tablets and smart phones issued without encryption, authentication or anti-malware software.

Yet those new devices are more powerful than were early laptop PCs, and are far more tightly connected to business-critical systems, via the internet.

And organisations are failing to take simple but vital security steps, such as asking developers to provide security certification for their applications, or insisting that staff use complex passwords, and change them often.

Look at the business as a whole, not in part, says PA expert Rupert Chapman

"The only reason passwords are vulnerable is because we're using the same passwords over and over again," warns John Pescatore, a vice-president at Gartner, the analysts. Yet that is exactly what too many users, and businesses, still do.

But some organisations that are using security to their advantage.

Prescott Winter, a former chief technologist at the US National Security Agency, and now chief technology officer at ArcSight, an HP company, says: "We used to say at NSA that security was bolted on. That has changed, mercifully, and there are quite a few companies that are doing a good job at security."

"And companies that do security very well, say that it is a business enabler rather than a cost," he says. "It furthers their mission or engages customers more effectively and with greater confidence, if they pay attention to security."

Fraudsters thrive in a parallel web universe

Malware economy

Criminals rival Silicon Valley in development of business models, says **Joseph Menn**

If you have ever received a message from a friend on Facebook, MySpace or Bebo recommending a hidden-camera video, you've probably had a brush with the most modern of crimes.

Such links typically lead to pages requiring an updated version of what is supposed to be the ubiquitous Flash video player. One click on the word "install" infects a user's computer with malicious software.

Until a sophisticated crime gang's unpublicised takedown earlier this year, the software was probably the one known to security professionals as Koobface, an anagram for Facebook.

Before Koobface was largely cut off, Nart Villeneuve, a University of Toronto researcher, won access to some of the servers at the centre of the operation. What he found there helps show how criminals – who years ago displaced porn purveyors at the cutting edge of technology – might now rival Silicon Valley in the development of new business models as well.

The two partners who ran Koobface controlled 21,790 Facebook accounts with nearly 1m friends and enjoyed 500,000 Google logins as well. What is most striking about Koobface is not how much money it took in – $2m in the year ended last June is a tiny sum, considering how pervasive its wares were – but how complex and flexible it all was.

The Koobface crew eschewed direct theft of financial account numbers and passwords, apparently realising that doing so would bring faster attention from the social networks and law enforcement.

Instead, the group allied with two types of fraud operations, performing crime as a service. At least seven clients paid the Koobface duo a total of $1m in commissions for steering captive PC users to bogus security software, one of the most profitable parts of the cybercrime trade. Such software pretends to find infections, demands credit card numbers for payment, and installs still more malicious codes.

The second set of fraudsters was in the pay-per-click business. At least 11 companies gave the Koobface operators a total of $1m to install software that would capture users' clicks on search results or ads on Google, Yahoo or Bing and send them off to brokers who resold the traffic, often back to the search engines that should have received the clicks in the first place.

Such schemes often earned as little as a penny or two per click, but security firm Trend Micro found a similar hijacking operation earned as much as $2 for each click on such valuable phrases as "home-based business opportunities".

While Koobface's low-impact operation might have been designed to avoid law enforcement, more flagrant criminal escapades likewise rely on shifting networks of allies that allow rapid changes in pursuit of bigger money.

To further reduce the low odds of capture, they use geographical boundaries, opaque business structures and specialisation.

Increasingly, the authors of a piece of particularly effective malicious software will not infect machines themselves. Instead, they will sell their programs to others, which reduces their risk because in most jurisdictions that it is not by itself a crime.

Other innovations include licensing the tools of the trade, which come with high-end rights-management locks to prevent unauthorised duplication, and auction sites that distribute to the highest bidder "exploits" for breaking into specific software.

"Their economy is booming and still evolving and becoming more complex," says Don Jackson, a researcher at SecureWorks. "There are more roles for service providers and value-added players. It's a very raw form of a very free market."

Much of the underground commerce occurs over encrypted instant message chats or on password-protected forums that are open only to aspiring members who come recommended by two or more veterans of the bazaars.

Made in China: counterfeit drugs such as these are often sold via Russia to consumers in the west Bloomberg

Credit card account numbers are the most common items for sale, says Symantec, the largest security firm, with prices as low as 7 cents each in bulk. Next in popularity are bank account particulars, which can fetch nearly $1,000 depending on the available balance and other factors.

Criminals can rent time on 'botnets', or networks of compromised 'robot' computers

To deal with the trust problems of doing business with unknown parties, forum members give feedback like that on Ebay. Intermediaries also offer escrow services to ensure the goods or services are delivered as promised.

Criminals can rent time on "botnets", or networks of compromised "robot" computers, and hire cash-out experts who in turn recruit "mules" to launder money from compromised bank accounts by making transfers abroad.

A fast-growing part of the economy is the "pay-per-install" industry. Those sites connect hackers who have access to PCs with people that want their malicious software installed.

One of the biggest cash generators in cybercrime – worth in excess of $100m a year to large participants – is the trade in counterfeit and unlicensed pharmaceuticals. The mini-economy of online drug sales among other things produces more than half of all e-mail, according to Symantec – more than three-quarters, according to some.

The manufacturers of the drugs are often in China or India, while the sellers are in Russia and the customers in the west. Police have been thwarted for years because of varying national laws.

A recent rift between two Russians has exposed more of the business. Igor Gusev and Pavel Vrublevsky were co-founders of ChronoPay, one the largest Russian online payment processors, and the latter remains the top officer there.

Amid a dispute between the pair, Mr Gusev has been charged by Russian authorities for allegedly unregistered involvement with one of the largest pharmacy networks, GlavMed. Mr Gusev has retaliated by distributing documents apparently tying Mr Vrublevsky to Rx-Promotion, a big pharmacy accused by the US Food and Drug Administration of offering dangerous drugs without prescription.

Mr Gusev has denied wrongdoing – his lawyer Vadim Kolosov has said he is innocent – and Mr Vrublevsky says he has never owned a stake in Rx-Promotion, adding that such companies generally operate elsewhere, shielding them from Russian laws.

All the same, Russian authorities have reopened a dormant probe involving Mr Vrublevsky.

Defences are boosted to fight e-crime

Country profile
UK

Three-pronged plan is immune from spending cuts, says **James Blitz**

The UK has faced immense challenges in the field of defence and security in recent times, with prime minister David Cameron's government forced to slash defence spending because of the country's fiscal crisis.

But, while much of the ministry of defence may be squealing about these moves, the government has been keen to ensure that one area of Whitehall expenditure continues to grow: cybersecurity.

In last October's review of defence strategy, Mr Cameron said the UK's cybersecurity budget would grow by some £650m ($1.05bn) over the next four years. The increased cash is an acknowledgement of just how seriously the cyber threat is being taken in Britain today.

William Hague, the UK foreign secretary, spelt out in February this year why the government's concerns have risen. He told the annual Munich Security Conference that e-crime attacks on private-sector companies were becoming a serious concern.

Intelligence reports that he had seen showed that just one criminal computer program can harvest more than 30 gigabytes of stolen passwords and credit card details from more than 100 countries in a matter of days.

The UK government is also alarmed at how its own systems are coming repeatedly under attack.

Last December, government computers were targeted by Zeus, a well-known piece of malware, that attempts to steal banking information and other personal details. A large number of e-mails bypassed government filters.

This year, a hostile state intelligence agency – almost certainly Chinese – attacked computers belonging to three members of Mr Hague's staff. The attack was undertaken by despatching an e-mail that contained an attachment with a computer code that would have invaded their machines. Fortunately the government's automated systems stopped it getting into the machines.

Given the scale of these threats, what is the UK's overall strategy on cybersecurity? Whitehall officials say their agenda essentially comprises three key strands.

The first is the need to improve co-ordination across government departments and agencies. There is a wide range of government actors involved in maintaining cybersecurity, such as GCHQ, the government's listening post; the Home Office, which is responsible for domestic law and order; and the intelligence services MI5 and MI6.

To help co-ordinate all these, a body called the Office of Cyber Security and Information Assurance has been set up. It has a staff of about 30 to ensure that the correct standards and procedures are being used across Whitehall.

The second strand of policy is to boost the UK's core cybersecurity capabilities. GCHQ clearly plays a critical role in ensuring that the UK is aware of potential threats emerging in cyberspace. Whitehall officials believe the agency is at the cutting edge of intelligence work in the communications and cyber field.

But the UK has also established a new Defence Cyber Operations Group, which incorporates cybersecurity into the mainstream of UK defence planning more generally. Dcog provides a cadre of experts that can support cyber operations by the Ministry of Defence, ensuring that vital government networks are secured.

The third strand of UK activity in this field is broad policy. The UK, along with other western states, wants to try to get governments to agree norms of acceptable behaviour in cyberspace, drawing up a convention restricting states or state-sponsored actors from carrying out disruptive attacks.

The government is alarmed at how its own systems are coming repeatedly under attack

To that end, the UK is to host a conference in London this November at which it wants to thrash out what such agreed norms might be.

UK officials acknowledge that getting states to agree on a common set of principles will be difficult.

China and Russia are pressing for an agreement but want something that will heavily regulate content in cyberspace.

The US and UK suspect that China and Russia are motivated by a desire to restrict internet freedoms. As a result, they want a loose convention that can set out benchmarks of good behaviour and put moral pressure on states not to undertake aggressive attacks.

Whether such agreement can be reached is far from clear and many would say highly unlikely. But UK officials are hoping that China and Russia will be at the November conference to engage in the debate.

As one Whitehall official puts it: "We cannot have a serious conference without ensuring there is a frank and open discussion with all the countries that you would want to have sitting at the table at a moment like that."

A god-awful problem – but the business model is divine

Malware profile
Zeus

Joseph Menn on a program that has kept international law enforcement busy for years

Perhaps no single piece of code illustrates the complex and costly challenges of cybersecurity better than a program called Zeus.

While there have been increasing cyber attacks on government assets for strategic reasons and private companies for their trade secrets, the most widespread incidents of criminal hacking are still about money.

In that quest, Zeus has reigned as a god of gods for years, with the FBI crediting a single ring wielding the program for the theft of $70m.

And that is just what law enforcement thought it could prove, says researcher Don Jackson of Dell SecureWorks, who has worked with the FBI and banks studying Zeus for years. "In its lifetime, Zeus has probably stolen $1bn," he adds.

Zeus is so pervasive and effective at stealing money from online bank accounts that it has prompted one of the largest international crackdowns by law enforcement in the history of cybercrime.

Late last year, authorities in the UK, US and elsewhere arrested scores of alleged Zeus "mules" – rank-and-file gang employees who were tasked with receiving transfers from compromised accounts and then passing them along to ringmasters elsewhere.

Those arrests, while not making much of a dent in an overall mule workforce in the tens of thousands, were unusual by themselves.

But the real coup came in Ukraine, which has a spotty record for co-operating in big cybercrime cases. There, national police working with the FBI arrested five alleged leaders of the ring. The Ukrainian government said charges could be filed within a week or two.

Unfortunately, the good news stops about there.

A Zeus-inspired review by US banking regulators of required security standards has dragged on in Washington, despite evidence that Zeus and similar malicious software can beat one-time passwords and other sophisticated defensive measures.

No charges have been forthcoming in Ukraine, although law enforcement sources say they are hoping that co-operation by one or more of the briefly detained group will yield dividends.

In the meantime, the author of the code remains free in his native Russia, where law enforcement co-ordination is even harder to come by.

Zeus most commonly infects consumers who visit a scammer's website or a legitimate page that has been hacked or unknowingly carries a malicious advertisement. It looks for any one of numerous flaws in the web browsers of the visitors to that page.

Zeus can be customised to go after accounts at specific banks or certain regions

Once inside a target's machine, it can hide itself in a variety of places and wait for the machine's owner to log on to a bank or other financial site, intercepting account numbers and passwords and sending them to the Zeus controller.

As technically impressive as it is, the most important thing about Zeus is the business model.

Older versions of the code are given away free. But users often upgrade to newer and better editions—the so-called "freemium" model that many smartphone applications also employ.

Zeus can be customised to go after accounts at specific banks or certain regions. A help manual and technical support are better than those for many legitimate pieces of complex software, according to F-Secure, a Finnish security firm.

The paid-for versions are licensed, and the technology enforcing those licences is state-of-the-art.

To make sure it is being run only from one approved machine, the program takes a snapshot of the unique identifiers on the chips, hard drive and elsewhere, and forms an encrypted digital fingerprint that has yet to be broken.

"The licensing scheme is as good as or better than any licensing system for commercial software," says Mr Jackson.

The website ZeusTracker, which has records of more than 1,700 active versions of Zeus, says 180 of them cannot be detected by any of the dozens of brands of commercial antivirus software. Another 540 are detected by 20 per cent or fewer.

Even worse are the ends to which Zeus has been put. Last year, one Zeus ring targeted individuals working in the US government and private industry on defence projects, using e-mails that appeared to have been sent by two prominent security researchers and urging the recipients to install what was marked as a fix for a flaw in Microsoft's Windows.

Those downloads brought Zeus to some 74,000 machines.

Web swoop: FBI special agent Weysan Dun announces arrests in New York, London and Ukraine in connection with a cyber theft ring that netted at least $70m AP

The Canadian SecDev Group found that this version of the program began stealing passwords and confidential documents, "including contracts between defence contractors and the US military, [and] documents relating to, among other issues, computer network operations, electronic warfare and defence against biological and chemical terrorism".

That operation suggests that a national government was a Zeus customer, says Will Gragido, a researcher at Hewlett-Packard's TippingPoint security lab, implying a level of patronage that makes it even less likely that Zeus will be stopped.

"It makes perfect sense. If you are in a professional criminal syndicate, the odds are you are not stupid, and your goal is staying employed", says Mr Gragido, a veteran of military intelligence. State espionage "is perceived as less risky in terms of prosecution and extradition".

Contributors

Joseph Menn
San Francisco Technology Correspondent

James Blitz
Diplomatic Editor

Tim Bradshaw
UK Digital Media Correspondent

April Dembosky
San Francisco Reporter

Chris Nuttall
San Francisco Correspondent

Maija Palmer
IT Correspondent

Stephen Pritchard, Jessica Twentyman
FT Contributors

Andrew Baxter
Commissioning Editor
Steven Bird
Designer
Andy Mears
Picture Editor

For advertising details, contact: **Liam Sweeney**
Telephone +44 (0)20 7873 4148; e-mail: liam.sweeney@ft.com