CYBERSECURITY

Legal Business
September 2013

KNOWN UNKNOWNS

Combating cyberattacks on law firms is complicated by the lack of hard information and the shadowy nature of perpetrators. But, reports *Legal Business*, law firm tech chiefs and security specialists agree the threat is rapidly growing

JAISHREE KALIA

What is a law firm if not a huge repository of commercially valuable information? On one side, of course, is the vast bank of specialist legal information held by experienced staff and databases of precedents and legal know-how. Yet valuable as that intellectual property (IP) is – it's very hard to steal legal expertise.

It is a very different story for the other major tranche of information law firms hold, that of their clients. A major international law firm will typically manage more than 5,000 sizeable clients at a time, covering major companies, governments and high-net-worth individuals. The combined economic power of a client portfolio of a single top-tier law firm is huge – running into trillions of pounds and legal professional privilege means that an external adviser is often seen as a natural place to store sensitive material.

Put in that context, it is easy to see why there is a growing body of opinion that law firms will increasingly be a prime target for a large and growing number of organisations and individuals looking to break into their security.

In an age where such espionage is conducted online and international law firms have to conduct business across a wide array of states, while deploying a broad range of online tools, we have certainly moved on hugely from the quaint old days when the biggest security concern facing law firms was odd individuals or private investigators rifling through their bins.

Simmons & Simmons chief technical officer Peter Attwood says: 'Banks are highly regulated and have very secure systems. If hackers can't break into the banking systems then they look to those professional services organisations that receive a flow of information from the bank such as law firms.'

'We are targets for our client information,' agrees Doug Twining, head of information systems strategy and planning at Linklaters.

Additional factors have put cybersecurity further up the agenda, including the rapid growth of interlocking data security laws that have been introduced in the US and Europe over the last decade, many of them ushering in obligations on companies to protect client data and to notify regulators of serious breaches. This is particularly prevalent in the US, where enforcement agencies like the Federal Trade Commission have pursued companies that suffered security breaches for failure to comply with relevant legislation. ▶

Illustration SHUTTERSTOCK

‘If hackers can’t break into the banking systems then they look to those professional services organisations that receive a flow of information from the bank such as law firms.’

Peter Attwood, Simmons & Simmons

▶ The Boardroom Bellwether survey from the Institute of Chartered Secretaries and Administrators, an organisation specialising in governance and compliance, found four in five companies are not prepared for cyberattacks and 80% of boards are failing to take cyber risk seriously. In addition, data from RSA, the security division of IT and data storage provider EMC, concluded there has been a marked increase in high-impact cyberattacks in recent years.

By consensus, general counsel have also begun to push advisers to provide more information on security measures and to demonstrate they can fit in with internal policies on data protection deployed at bluechips.

With chief information officers (CIOs) looking to bolster their defences, *Legal Business* decided to assess the current risks of cyberbreaches and find what steps can be taken to mitigate the risks. We also try to identify who these hackers are and what some of their sophisticated hacking tricks look like.

KEEPING THE GOLDEN EGGS

Chris Andrews, director of risk management at Simmons & Simmons, says law firms are at most risk in two areas: mergers and acquisitions (M&A) and intellectual property (IP). He says in terms of corporate takeover work, there could be a bid or price-sensitive data that is of interest, while in IP, there is a perception that commercially useful information will be stored, such as the proverbial Coca-Cola recipe. Additionally, recent information from the Centre for the Protection of National Infrastructure (CPNI), the UK government-backed agency that provides security advice to businesses, concluded that the banking, energy and pharmaceutical sectors are prime targets for hackers.

According to Peter Tran, senior director of advanced cyberdefence services at RSA, IP advisers are seeing a significant rise in state-backed snooping. ‘These firms are the keepers of the “golden eggs” for their clients and have trust established with their client-base so it would make a great hot-point to exploit a client’s network via their law firm,’ he explains.

Tran also points out that beyond traditional target areas like energy, defence, banking and life sciences, there has been an increased trend in attacks toward supply chain, logistics, manufacturing, retail and professional services firms, especially within advisory and audit and IP.

Providing a different perspective, Berwin Leighton Paisner (BLP) director of IT Janet Day says law firms are increasingly likely to be targeted for specific client teams. ‘It’s not a particular practice area that is at risk. I think it’s more likely to be a client team because the client themselves is at risk, and many firms will act in multiple sectors for a client,’ says Day.

KNOW YOUR ENEMY

There are different groups of hackers with very different goals. One group is state-sponsored or semi-state-sponsored individuals who extract secrets. This is where an individual is sponsored by a government for the purpose of either classic espionage – such as spying on terrorists or foreign governments – or industrial espionage such as hacking into a company to find its secrets so they can be utilised for strategic or commercial interests.

There is some overlap in the two definitions as breaking into corporate systems for ▶

- Fraud
- Bribery & Corruption
- Information Security & Cyber threats
- Asset Tracing & Recovery
- Litigation Support
- Dispute Resolution
- Forensic Accounting
- Transaction Intelligence

Your Global Investigations Partner

Kroll's Investigations team contains a unique mix of specialised skills. We work in small multi-skilled teams to deliver customised investigations which produce evidence that meets the highest litigation standards. Around the world we enable our clients to make informed decisions about their most difficult challenges.

Our team includes intelligence gathering, law enforcement,accountancy, data analytics and cyber investigation expertise.

+44 (0) 207 029 5000 | KrollUK@kroll.com | www.krolladvisory.com

Kroll®

information about a nuclear weapon, for example, would fit into both categories.

'When we observe the activities and the attacks that are going on, it is clearly not just some spotty-faced teenager sitting in his parents' garden shed. These are industrialised operations with multiple layers of command and hierarchy that actually operate as a day job,' says Tom Burton, head of cybermanaged security services at international business and technology consulting firm BAE Systems Detica. 'In one recent attack, which was strongly believed to have originated from Russia, all of the activity, in terms of codes being compiled and infrastructure being stood up, occurred between Monday to Friday between the Moscow time zone of 8am to 5pm and with no activity in the evenings and the weekends. It's very much a day job.'

'Law firms are taking the lead from what governments are saying from the developing consensus regarding the threats and risks.'

Daniel Pollick, DLA Piper

A second group are essentially organised criminal gangs, which are typically hosted abroad, that are seeking to steal information that can be converted into money. Target information for this type of group is credit card and bank account numbers.

For example, in May 2013, a gang of cybercriminals cashed in on $45m from two Middle Eastern banks in a matter of hours in one of the biggest heists to hit financial institutions, by hacking into a database of prepaid debit cards and then physically spreading around the globe to drain cash machines.

In essence, the business of cyberespionage has rapidly evolved into a highly organised activity with hubs of specialist criminals and hackers emerging in centres like Shanghai and Kiev, some of whom are stealing targeted information to order.

Benedict Hamilton, a managing director in Kroll's global investigations and disputes practice, says: 'Cyberespionage – that is state-sponsored and sophisticated – typically begins with in-depth, open source research and highly sophisticated attack vectors. India and other countries are joining those that have long been established in this area such as the US, the UK, Russia, China, Israel, Iran and North Korea.'

Seth Berman, executive managing director at global digital risk management company Stroz Friedberg, says: 'This type of criminal activity is done by the modern equivalent of the Mafia. They are organised in a very different way to the Mafia, but they are groups of people working together to get money however they can do so.'

A third group are internet activists known as 'hacktivists', who are classified as individuals that bear grudges against companies, countries or governments. 'Often-times they are simply trying to embarrass the company and give the business bad publicity rather than stealing any data,' adds Berman.

In April 2011, the internet hacktivist group known as Anonymous launched a series of attacks against Sony in retaliation for trying to stop hacks of the PlayStation 3 game console. More than 100 million Sony accounts were compromised and the Sony services Qriocity and PlayStation Network were taken down for a month by cyberattacks.

The fourth type of group consists of employees and former employees. These are insiders who effectively use the company's systems to steal information. Typically, this could be an employee that is leaving and joining a competitor. While these are not hackers as they already have access to the systems, they are in any event abusing their access.

CYBERCOMBAT CHECKLIST – THE SPECIALISTS' TIPS TO PROOF YOUR SYSTEM

1. Protect your perimeter
2. Review your firewall protection regularly
3. Use penetration testing – employ specialists to try to break into the system and plug defects immediately
4. Monitor what is being downloaded and put controls on how much data can be downloaded in a single instance to help identify unusual activity
5. User education – educate your staff on what spear phishing looks like, get employees involved and let them know what the risks are, where they will be targeted and how to deal with them
6. Know your employees – use robust pre-employment screening
7. Assign members of the in-house legal team to review policies and enforcement to assess legal risk
8. Enforce policies – ensure employees change password every month
9. Ensure security covers homeworking, BYOD and remote media
10. Review your insurance protection

Attwood at Simmons comments: 'Often it's not technology but an inside job. A disgruntled employee who is being bribed should not be discounted in the electronic ages. While historically a few pieces of paper were photocopied, now a wealth of information can be downloaded onto a USB stick.'

HUMAN WEAKNESS

Hackers use a wide range of methods to exploit the gaps in company systems while taking advantage of staff to get into systems from the

inside. Berman says law firms are increasingly being targeted because of the way they are structured. 'There are lots of ways to access the systems in law firms. They have flat structures because numerous users need access quickly as opposed to in banks, this leaves them open to more cyber risks,' Berman says.

So how do hackers get in? One common form of sophisticated hacking is dubbed spear phishing, a highly targeted and refined version of phishing, which is aimed at a niche group of people. While a phishing e-mail is sent out to multiple users with the hope that one will click, with spear phishing a lot more time is spent creating a highly believable story designed to get a specific individual to click.

'It is not that hard to carry out research on a lawyer. Websites show where they went to school, which firms they have worked for and what cases they have worked on. From this, a hacker can craft an incredibly believable e-mail,' Berman warns.

Stroz Friedberg saw a recent case at one mid-tier law firm where every associate was sent an e-mail that looked like it was from a senior partner where the e-mail requested associates click on a document for a meeting the following day. In this type of case, the likelihood of an associate clicking is very high. To the disadvantage of the hacker, so many associates clicked on the e-mail that the problem was identified and dealt with before any virus was inserted.

Other vulnerabilities include poor perimeter control where firms expose internal systems online by default after installation, poor password control and human engineering, where documents with viruses are opened on firm devices allowing the hacker access into the firm's internal systems as well as the users' personal information, such as contact lists.

Other instances include a forced password change, where lawyers are sent copy e-mails of the original host requesting they change passwords, which not only provides full access to the hacker but also locks the user out of its account.

In some cases, infected USB sticks get planted in multiple firms which when inserted downloads a piece of software that opens an internal channel. 'It is much easier for a virus to operate from inside a firm and send information out rather than attack directly from outside,' says Attwood.

While top-flight law firms are often being targeted, hackers are showing an increased interest in second-tier advisers where in some cases the hacking has gone unnoticed by the firm until the client itself has been hacked or in other cases where sensitive information has leaked.

'Clients have become much more demanding in terms of how their information is protected and are becoming increasingly detailed in audits.'
Doug Twining, Linklaters

Stroz Friedberg had a recent case where information in relation to a celebrity case was leaking from a law firm. In this instance, the law firm approached Stroz Friedberg to try to identify how this information was leaking.

The type of attention a firm receives depends to some extent on its clients. 'Is a small matrimonial law firm that specialises in divorce issues at a lower risk in comparison to a Magic Circle firm? Probably; it will have a lower risk of state-sponsored attacks but a much higher risk of litigant attacks,' says Berman.

Another key issue for law firms to consider regarding security is the implications of using remotely hosted cloud computing, a topic which continues to divide opinion in the legal profession. While conservatives worry about the vulnerability of data held in remote servers, an increasingly sizeable group of IT professionals maintain that the larger providers at least have regularly-upgraded security systems that are considerably more robust than most law firms.

Kroll's Hamilton says that data can be further safeguarded by having legal agreements with cloud providers to allow forensic investigation after an event such as a security breach.

GETTING PROTECTION

DLA Piper CIO and head of IT Daniel Pollick argues that in 2013 legal advisers should have two prime aims: costs and security. 'Law firms are taking the lead from what governments are saying and from the developing consensus regarding the threats and risks. Firms need to invest serious effort and money into cybersecurity to understand and address their vulnerabilities,' he says.

Simmons' Andrews says its firm has not been a victim of cybercrime yet but it could only be a matter of time. The firm reviews its firewall protection regularly and employs specialists to try to break into its systems so they can plug any defects. While a lot of the threats are externally posed, Andrews says the internal risk remains substantive.

'A firm's data is as secure as a firm's pre-screening per each individual being employed,' warns Andrews. 'Firms need to focus on having robust pre-employment screening processes.'

According to Twining, Linklaters was one of the first firms to use an advanced monitoring capability to identify covert activity. Previously, a malware – a programme used by hackers – attempted to break into Linklaters' servers but was unsuccessful.

Twining joined the City leader in October 2011 from BP where he was head of programmes and change. Last year he went to Linklaters' management with a proposal to spend more on security. 'The executive committee understood the problem straight away which was great – it is very powerful when you obtain endorsement from senior leaders.'

He also set up a security programme to help the firm keep up to date with any developments in the cyberworld, monitoring who the new players are and what the firm needs to mitigate against. 'Every firm needs a targeted approach. In the past we had hacktivists, state players and organised crime acting separately. Now, these groups are teaming up and they have huge resources at their disposal,' he says.

BLP's Day says firms need to educate users to minimise the odds of falling victim to cyberscams. Firms should also employ penetration testing to monitor target hacks. ▶

‘Cyberespionage – that is state-sponsored and sophisticated – typically begins with in-depth, open source research and highly sophisticated attack vectors.’

Benedict Hamilton, Kroll

‘The systems at BLP are as secure as we can make them but individuals are capable of doing things with intent as well as inadvertently,’ she adds.

RSA’s Tran says investments into securing systems are typically scrutinised by law firm partners as it is an expense. ‘This mind-set is changing, however, as firms see how sophisticated attacks are evolving, particularly as attackers are using multiple targets and vectors to attain their objectives.’

THE BYOD DILEMMA

While some firms have side-lined security it is clear that clients have not. ‘Clients have become much more demanding in terms of how their information is protected and are becoming increasingly detailed in audits. They are asking carefully structured questions and are specifying security controls,’ comments Twining.

He also emphasises the importance of client engagement on these risks. ‘One banking client requested Linklaters to put costly software in place to control network access. Once we understood the risks they were trying to manage, we suggested other controls, which managed this risk but were more suited for our infrastructure,’ says Twining.

Firms that employ a bring your own device (BYOD) policy have additional challenges to manage as it is harder to separate business phones and tablets from personal devices. There is no doubt that the rapid rise of BYOD over the last five years presents one of the most immediate security challenges to law firms.

Attwood comments: ‘Mobiles connected to law firm systems can contain viruses – they are a threat.’ Burton says that mobiles could be used provided the risk is managed. He says that rather than categorically barring lawyers from using their own mobile devices at work, law firms should use structured approaches to mitigate risks, such as monitoring mobile traffic and ensuring employees are using the minimum security standards for each device.

In terms of investment, Simmons’ Andrews says the firm has not increased investment into security but is currently reviewing its internal processes and insurance protection. ‘If client data was stolen, then professional indemnity (PI) insurance may cover it, but if a staff member’s data was lost through a raid, for example, then the firm may not be covered. So firms need to consider where the possible losses will be. There are bespoke cyberinsurance policies available and firms are increasingly looking into this,’ says Andrews.

For Linklaters, keeping up to date with any regulation that affects its clients is important in terms of enforcing security, while BLP’s Day says that lawyers are happy to use policies to guide them, provided they make sense.

The International Legal Technology Association was set up in the US around 25 years ago for law firms to discuss best practices in technology. Day says this, alongside the CPNI and the Solicitors Regulation Authority, provides the best support for advisers in forging effective policies on data security and use.

But there are also issues with policy enforcement. As Andrews points out: ‘Can you be confident the new office in Kuala Lumpur is adhering to policy compliance? The culture of a firm helps policy enforcement but the more firms grow, the more diverse they get and this can be problematic. For example, one firm may have a different mind-set to another that has been exposed through cyberattacks.’

Such tactics are seen in some countries where states are perceived as likely to seek out sensitive corporate information, in particular China. In one notable example, the recently merged King & Wood Mallesons separated off its IT system between its legacy Chinese and Australian partnerships to help manage this issue.

‘You can ring-fence off higher risk but this becomes a business barrier as clients want a single system platform, but developing one internal firewall is challenging,’ Andrews adds.

Day has a similar view: ‘[Law] firm mergers pose a serious problem in terms of cybersecurity. It needs time and work. There is a compliance issue and in some cases technical walls are put into place so lawyers in firm number one cannot access the systems in firm number two.’

THE LONG RUN

If cybersecurity is a risk that law firms have historically taken lightly, DLA’s Pollick believes a shift will emerge in the next few years. ‘At

present, this space is premature and firms will be resistant as it's an early stage,' he says.

But many law firm CIOs expect attitudes to change quickly. According to RSA's Tran, cybercriminals and hackers are increasingly forming established networks globally to co-operate. The attackers form partnerships, subcontract relationships and leverage exploitation techniques, tactics and procedures (TTPs).

'Typically you will find a wide web of hackers from nation state-sponsored, traditional cybercrime and others who have what is known as "collection requirements" much like a war board,' says Tran.

Twining comments: 'The Federal Bureau of Investigation and MI5 tell us about how some governments try to place dormant malware into firms' systems that are later activated and used for years without being detected. This shows they are in it for the long run.'

In June 2013, newspaper headlines were dominated by the row over online surveillance techniques used by governments in the US, Australia, UK and France to spy on domestic and international communications. The initiative saw the US National Security Agency (NSA) operate a complex web of spying programs that allowed it to intercept internet and telephone conversations from over a billion global users. It was revealed that many of the NSA's programs were aided by national and foreign intelligence services, including Britain's Government Communications Headquarters (GCHQ) and Australia's Defence Signals Directorate (DSD). The NSA also reportedly tapped into the servers of large private telecommunications and internet corporations, such as Google and Facebook.

Twining comments: 'State secrets and IP from UK PLCs are being systematically stolen. Therefore, the economic prospects can be compromised, so I can see the argument for some sort of monitoring. The flip side is issues on privacy and deception.'

Ultimately, wherever technology brings rewards and new tools it brings fresh challenges and ethical considerations. As BAE's Burton concludes: 'While these [changes] benefit society and the economy, they also benefit the less ethically pure. We need to reset the clock and rebalance by investing in improving our defences and awareness.' **LB**

jaishree.kalia@legalease.co.uk

Legal Business would like to thank Kroll for its sponsorship of this piece.

ON THE AGENDA THE CLIENT PERSPECTIVE ON CYBERSECURITY

If law firms have been relatively slow to wake up to the realities of cybercrime, there is considerable evidence that clients and general counsel (GCs) have become increasingly sensitive to the issue. Research from FTI Consulting of 1,957 GCs and 11,340 corporate directors last year found cybersecurity and data protection was ranked as one of the group's most pressing concerns, a sharp rise on equivalent surveys conducted five years previously.

Likewise, Winston & Strawn's 2013 International Business Risk Survey found that two-thirds of multinationals rated client data security and related risk issues as the most important data privacy challenge. The survey also found that companies were more concerned about suffering reputational damage in the event of a data breach in comparison to regulator sanctions.

Awareness of the issue certainly varies considerably by region, with US-based companies, which face the greater threat of regulatory action or follow-on litigation, typically well ahead of counterparts in Europe.

This differing attitude was underlined in 2011 when the US Securities and Exchange Commission went as far as to issue disclosure guidance to listed companies in relation to cybersecurity incidents. In context, companies in major emerging economies like China and India are generally relaxed about tech security compared to Western equivalents.

Craig O'Donnell, head of information systems at property group Land Securities, comments: 'Last month we blocked 42,000 attacks at our web gateway. If you don't have security, you are extremely vulnerable.'

However, O'Donnell argues that the majority of attempted breaches can be dealt with by ensuring fairly basic measures are in place, such as encrypting sensitive data and e-mails, implementing standard security around homeworking and removable media like USB sticks and raising staff awareness on security issues. He also advises companies to take a realistic view about how important the various data being held is and to form policies accordingly, commenting: '80% of cyberattacks can be mitigated by basic risk management.'

However, while IT professionals are clearly alive to the threat, in-house legal teams in the UK still often rely on their in-house tech teams or law firms to protect data, despite a general unease with what many GCs see as relatively loose terms on security in standard engagement letters.

Ruth Daniels, GC of outsourcing company CPA Global, comments: 'GCs need to be asking more of their law firms around technical security. GCs should be looking at provisions of terms of engagement with law firms.'

Philip Price, chief operating officer at Arle Capital Partners, comments: 'For us it is a bit like dealing with any other regulated entity. When I deal with FCA-regulated entities, I take a lot of comfort from the fact they have FCA oversight of their activities. With law firms I think it is fair to take the view that if the SRA is involved and has oversight you would expect minimum standards in relation to client confidentiality and by extension [cyber] security measures.'

Daniels: GCs must ask more from law firms regarding technical security

Specific steps that GCs can take to manage legal liability in the event of a breach include creating or reviewing a documented cybersecurity policy to demonstrate that the company understands and has taken effective steps to protect its data.

A recent report from Hogan Lovells also recommends a range of measures, including having legal input into cybersecurity programmes and assigning members of the in-house team to the area. Other steps include updating due diligence in takeovers to address data protection and reviewing major contracts to assess potential liability in the event of a breach. Companies can also obtain far more robust cyber risk insurance than was available even as recently as the mid-2000s.

Land Securities' O'Donnell concludes by arguing that major companies should be willing to validate the security policies of third-party suppliers and legal advisers. '[When] we enter into an agreement or make demands on law firms that we work with, we actually test them to make sure they've got the right controls in place for what they've contractually signed up to do.'

Trust, it seems, will increasingly have to be earned.

Cyber-threats and the enemy within

Kroll's EJ Hilbert highlights the risks of cybercrime and outlines what firms can do to improve their security

Who is responsible for protecting your business from cyber-threats? Historically, this responsibility has often been delegated down the chain to an individual or group of individuals who are already over-worked trying to keep the IT systems up and running, and who have very limited knowledge of the methods of 'cybercrime'.

Does the person responsible know exactly what 'cybercrime' is? How would they know if your company's systems or information had already been compromised by a covert hacker or rogue employee?

Cybercrime is broadly defined as the use of a computer or computer network to conduct a criminal act motivated by some form of profit, usually monetary, or some other gain. This includes a variety of offences including identity theft, fraud, stalking, online extortion, spamming and phishing.

Kroll's 2012/13 Global Fraud Report reveals that 1 in 5 businesses (21%) suffered information theft, loss or attack over the previous 12 months. Of those companies that suffered an attack, 17% said their systems had been targeted by an external hacker and 5% had a vendor or supplier's systems hacked by an external party. Over a third (35%) of firms affected had suffered an incident stemming from employee misconduct.

It's often the attacks from external hackers that get picked up in the headlines, but in many cases the greatest threat to companies comes from within. In over 15 years spent chasing cybercriminals and helping victimised companies, be it with the FBI or in private industry, more than 60% of the cases that I have worked on involved internal employee actions.

Statistics only go so far in describing the severity of risk caused by a diverse range of cyber-threats. Real-life examples paint a more complete and persuasive picture, and such examples abound in the record of federal prosecutions. In the US, the FBI doubled the number of trade secret arrests in the last four years and the overwhelming majority of those prosecutions involved insiders.

> **'In over 15 years spent chasing cybercriminals, more than 60% of the cases that I have worked on involved internal employees.'**
>
> EJ Hilbert, Kroll

CASE 1: ECONOMIC ESPIONAGE

On 21 December 2011 in the US District Court for the District of Indiana, defendant Kexue Huang was sentenced to seven years and three months' imprisonment after his conviction on charges of economic espionage and theft of trade secrets. The charges principally concerned the theft of trade secrets related to a commercial insecticide developed by Dow Chemical Company in Indiana, where Huang, a Canadian national, worked as a research scientist from 2003 until 2008, when he was fired. He admitted to stealing $300m worth of Dow trade secrets and delivering them to the People's Republic of China (PRC) and Germany through an intermediary. He used the trade secrets to conduct unauthorised research with the intent to benefit foreign universities that were instrumentalities of the PRC government. Huang also admitted that after he was fired by Dow, he went to work as a biotechnologist for grain distributor Cargill. Again, while employed by Cargill, he stole a trade secret involving a key component of a new Cargill food product, which he then gave to a student at Hunan Normal University in China. If there is such a thing as a serial malicious insider, Huang fits the bill.

At the time of Huang's guilty plea, the head of the FBI's field office in Indiana stated:

> 'Among the various economic espionage and theft of trade secret cases that the FBI has investigated in Indiana, the vast majority involve an inside employee with legitimate access who is stealing in order to benefit another organisation or country. This type of threat, which the FBI refers to as the Insider Threat, often causes the most damage.'

CASE 2: THE OPPORTUNIST

On 29 August 2012, Hanjuan Jin was sentenced to four years' imprisonment for stealing Motorola trade secrets. She had been a software engineer at Motorola from 1998 to February 2007. While on medical leave in 2006, Jin accepted employment with a Chinese competitor company, Sun Kaisens. She then returned to work at Motorola. At various times from 26-27 February 2007, Jin downloaded from Motorola's secure internal computer network numerous proprietary technical documents and removed several documents and other materials from the company's offices. Also on 27 February, Jin e-mailed her manager to give notice that she would be leaving Motorola immediately. The following day, she was arrested at Chicago's O'Hare Airport after purchasing a one-way ticket to China. Police found her in possession of more than 1,000 electronic and paper documents belonging to Motorola.

CASE 3: THE MOLE

In February 2010, Greg Chung, a former Rockwell and Boeing engineer, was sentenced to more than 15 years' imprisonment for acting as an agent of the PRC and stealing trade secrets about the Space Shuttle, the Delta IV rocket and the C-17 military cargo jet for the benefit of the Chinese government. In a September 2006 search of Chung's residence, FBI and NASA agents found more than 250,000 pages of documents from Boeing, Rockwell and other defence contractors inside the house and in a crawl space underneath the house. Among the documents were scores of binders containing decades-worth of stress analysis reports, test results and design

information for the Space Shuttle. Chung also sent numerous engineering manuals to the PRC, including 24 manuals relating to the B-1 bomber that Rockwell had prohibited from disclosure outside the company and select federal agencies.

CASE 4: THE DISGRUNTLED EX-EMPLOYEE

In March 2010, Michael Mitchell was sentenced to 18 months in prison and ordered to pay his former employer more than $187,000. Mitchell had soured on his job at DuPont as a Kevlar® marketing executive and was ultimately fired for poor performance. Before leaving, he downloaded numerous computer files with DuPont trade secrets and gave them to Kolon Industries, a South Korean competitor of DuPont's Kevlar® products with which Mitchell entered into a consultant agreement. In this case, however, there may yet be a happy ending for the victim – or, at least, a not so unhappy ending.

On 14 September 2011, a jury in the US District Court for the Eastern District of Virginia awarded DuPont damages in the amount of $919.9m. That civil judgment is on appeal. On 18 October 2012, the US Department of Justice indicted Kolon Industries and several of its executives and employees for engaging in a multi-year campaign to steal trade secrets related to DuPont's Kevlar® products. The indictment seeks forfeiture of at least $225m in illicit proceeds.

CASE 5 : THE DISGRUNTLED SYSTEMS ADMINISTRATOR

In December 2012, Switzerland's intelligence service (the NDB) informed its US and British counterparts of a major data theft by an NDB IT administrator involving terabytes of sensitive and classified data. The IT technician, an employee of eight years with administrative rights to most of the NDB network, became disgruntled because NDB management failed to implement his suggestions for improved systems management. He reportedly used his authorised access to copy huge amounts of intelligence data onto small portable drives, which he then smuggled outside in his backpack. He is believed to have tried to sell the data to third parties before he was arrested. The stolen material included classified data from both the British (MI6) and US (CIA) intelligence services.

So how can companies protect themselves from insider threats? Though the world likes to refer to a wide range of information security threats as being 'cyber', evoking images of a supercomputer operating without humans, the fact is all cyber-threats involve a human element for both attack and defence.

For a start, companies can enhance their profiling of employees most likely to commit cybercrimes. According to *CSO Magazine*'s 2012 CyberSecurity Watch Survey, 11 companies that experienced cybercrime by an insider in the previous 12 months reported that 51% of those insiders violated IT security policies and 19% were flagged by a manager for behaviour/performance issues.

> **Companies need to be fully aware of what information they have on their systems, who has access to it, who is accessing it and why.**
>
> EJ Hilbert, Kroll

The FBI's website (www.fbi.gov) provides a longer list of at-risk behavioural traits, including unreported overseas trips, seeking proprietary or classified information unrelated to work duties, paranoia about being investigated and disproportionate anger over career disappointments. When an employee leaves the company, voluntarily or involuntarily, strict termination procedures should be in place to ensure that all network access privileges are terminated immediately. While this may seem self-evident, it is remarkable how often it is overlooked or addressed too late.

Companies need to be fully aware of what information they have on their systems, who has access to it, who is accessing it and why. The concepts are data visibility, access control, monitoring and data lockdown.

Just as a company has security guards monitoring the parameter of a building, checking IDs, logging who enters and leaves the building and watching security monitors, the same precautions should be taken for data.

If Mary Jane is logged in from her work computer and the same credentials are used to log in from an external location, a red flag should immediately appear. If Joe Smith is uploading or downloading a large amount of data for the first time, those responsible for data security should be alerted.

This list of recommendations is by no means exhaustive, but highlights some of the practical steps that companies can take to mitigate the risk of insider threats.

Physical and logic security should be fully integrated into every company as well as business continuity/disaster recovery plans and regular staff training. Whether it's stemmed from a disgruntled employee, a mole planted by an organised crime gang or a sophisticated hacker, when an information security issue is discovered, an effective response plan needs to be activated. These plans should be constantly evolving and rigorously tested. Just as 'real world' fraudsters adapt the method of their attack, so do the cybercriminals.

Kroll®

FOR MORE INFORMATION

EJ Hilbert, managing director and head of cyber investigations, EMEA, Kroll

E-mail: ehilbert@kroll.com

Tel: 020 7029 5306

www.krolladvisory.com