LegalWeek Intelligence

The Unusual Suspects

Meet the biggest threats to your confidential data

In partnership with

Kroll

Kroll

Staying one step ahead of insider data leaks

Legal Week Intelligence in association with Kroll

Key findings

- Three in every four data breaches were **committed by a permanent employee** of the business in question, or a vendor with whom they were contracting.
- Over half of all data breaches **occur by accident**.
- Seventy five percent of breaches resulted from using workplace hardware or data outside the office environment.
- Businesses **fear losing client data** the most.
- **External campaign groups** are more feared than vendors even though vendors originated more breaches.
- A third of businesses contract **without provisions for how to proceed** in the event of a confidential data breach.
- Only **6 in 10 businesses** require the third party hosting their data to maintain a log of all events.

Methodology

Kroll's Information Security Study, conducted in association with Legal Week Intelligence, aims to investigate the issue of data breaches.
The survey was launched in mid-July 2015 and closed one month later in mid-August.
This research looks into several areas, including: the percentage of companies which have suffered data breaches recently; who the main perpetrators are; what types of information tend to be taken, and what sort of damage can result to those who suffer a breach.
The study also investigates what is being done to combat such threats and how these efforts can be improved upon.
Legal Week Intelligence canvassed the opinions of 86 general counsel and in-house lawyers from a multitude of industry backgrounds: most commonly from financial services. The vast majority of respondents were UK based, with just over half having additional operations in mainland Europe.

By Legal Week

Imagine the scene. A quiet company car park in which an employee — and not even a disaffected one — chances upon a USB flash drive marked 'bonuses'.

Their curiosity naturally gets the better of them and, thinking they have stumbled upon a tantalising company secret, they go to their office computer, load the drive and wait.

Within minutes they realise that the Excel spreadsheet it contains is full of incorrect data and can tell them nothing, but unbeknownst to them it has already told the hacker who planted it a great deal, for the memory stick is laced with software which grants them access to the company's IT system.

Whether the hacker is motivated by revenge, vandalism, personal gain, politics or anything else, some or all the company's innermost secrets will now be theirs.

All they needed was the unwitting help of an employee — and not even a disaffected one.

Benedict Hamilton, managing director of investigations and disputes at corporate investigations specialist Kroll, says this rogue USB trick was the example given to him by the tutor of a course he once attended.

Far from being an academic case, it is currently the second most effective way into a company's system, and would give the attacker access within two hours of them planting the USB.

So what's the most certain way in? According to that same tutor, a USB marked 'porn' would get an attacker inside the system in 20 minutes.

A business' IT staff might be alive to the potential threat of hackers, but are its lawyers — who are often privy to the most sensitive information and who play a key role in policing data use — being just as vigilant?

Legal Week Intelligence surveyed 86 general

counsel and other in-house lawyers from a multitude of industry backgrounds to gauge their approach to data security.

Asked whether their organisations had suffered a breach of confidential data in the past year, the vast majority of respondents (86%) said there had been no such data leaks at their organisations.

That's a remarkably high percentage and one which, on the face of it, might suggest that data breaches are a minority concern.

However, scratching beneath the surface reveals unsettling truths.

The consequences of a breach

Though a fraction of businesses admit to having had their confidential data breached, Legal Week Intelligence's survey also found that the nature and consequences of those breaches can be anything but small.

The findings show that client data is the type most commonly breached (75%), followed by employee details (50%) and company financial information (25%).

Losing data on one's own organisation is bad enough, but losing client data is arguably more harmful. Aside from being a blow to the reputation of one's business, it may also result in an action against the company by the aggrieved client.

Legal Week Intelligence's study found that the most common type of harm suffered as a result of a breach was a financial loss. In fact, 100% of these breaches took a toll on the balance sheet. However, the reputational damage and, in some cases, regulatory investigations which businesses also suffered show that an array of serious losses can lie in store, besides that of the data itself.

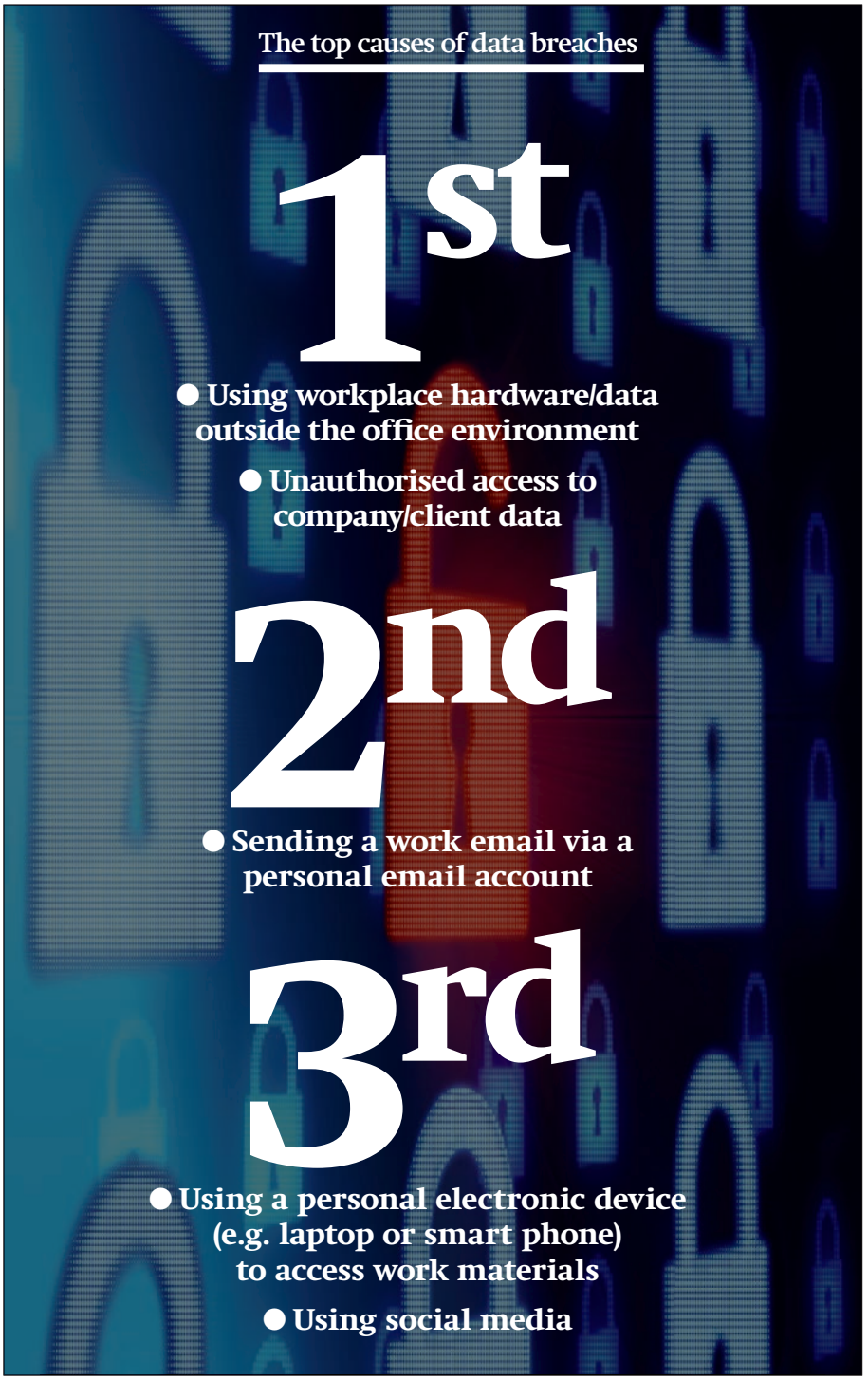
Know your enemy

Data breaches can be committed by many agents acting for many reasons: disgruntled staff, resentful former employees, negligent third parties, competitors seeking confidential data or intellectual property, or criminals acting for gain.

Against this hydra of threats, how can organisations effectively police their information borders? Legal Week Intelligence's survey suggests that businesses could begin by prioritising the protection of their most valuable data, and by

'A USB marked "bonuses" would get an attacker inside the system within two hours of it being planted'

Benedict Hamilton, Kroll



'Companies should know that there are many different ways in which attempts could be made, and I was surprised by the number [of respondents] that appeared not to be'

Paul Raymond, independent consultant

understanding where the real threats are coming from.

When asked which parties could cause the greatest damage, were they to commit a breach, external campaign groups were cited as being a much greater threat than third parties, vendors and privileged users (see right). However, in terms of numbers, third parties were involved in three times as many breaches as their hacktivist counterparts; and privileged users, twice as many.

This suggests the existence of a blind spot in corporate data security. "Companies should know that there are many different ways in which attempts could be made, and I was surprised by the number [of respondents] that appeared not to be," comments Paul Raymond, an independent consultant in financial services and data protection, who was formerly head of compliance at a leading insurer.

Another key misconception concerns motivation. Media coverage of recent high-profile data breaches has tended to concentrate on malicious assailants. However, our study finds that, although attempts to cause harm and financial gain both feature as key motivations behind breaches, the most common were the 57% which occurred by accident.

Respondents appear to associate data threats with the idea of malicious hackers working on laptops in darkened rooms. Our research suggests, to the contrary, that if businesses prepare only against external threats, they could leave themselves vulnerable to the greater danger posed by privileged users, vendors and other third parties.

The hidden attack vectors

Apart from cases of unauthorised access, the loss of sensitive data is most commonly caused when people use workplace data or hardware outside

the office environment — possibly arising from well-intentioned attempts to allow more flexible and remote working. Legal Week Intelligence's study found that a remarkable three in every four breaches follow from such incidents.

A second cause of data breaches is arguably a matter of attitude. Our research found that privileged users, including senior staff, were responsible for half of all breaches.

This echelon of management has access to the most sensitive levels of information on their respective organisations, but often these same individuals are the ones least likely to follow best practice guidelines for data security, on account of being too busy, unaware of the risks, or unaware of why such rules should apply to them.

Whatever their reasons, the consequences of senior management taking a lax approach to data security can be a ready source of embarrassment. Indeed, as Hamilton points out, this issue has recently had a direct bearing on Hilary Clinton's presidential campaign. Details recently came to light of her having used a personal email account for government matters while serving as Secretary of State.

So how can businesses better protect themselves against threats that are internal as well as external, and cultural as well as political?

PREVENTING THREATS

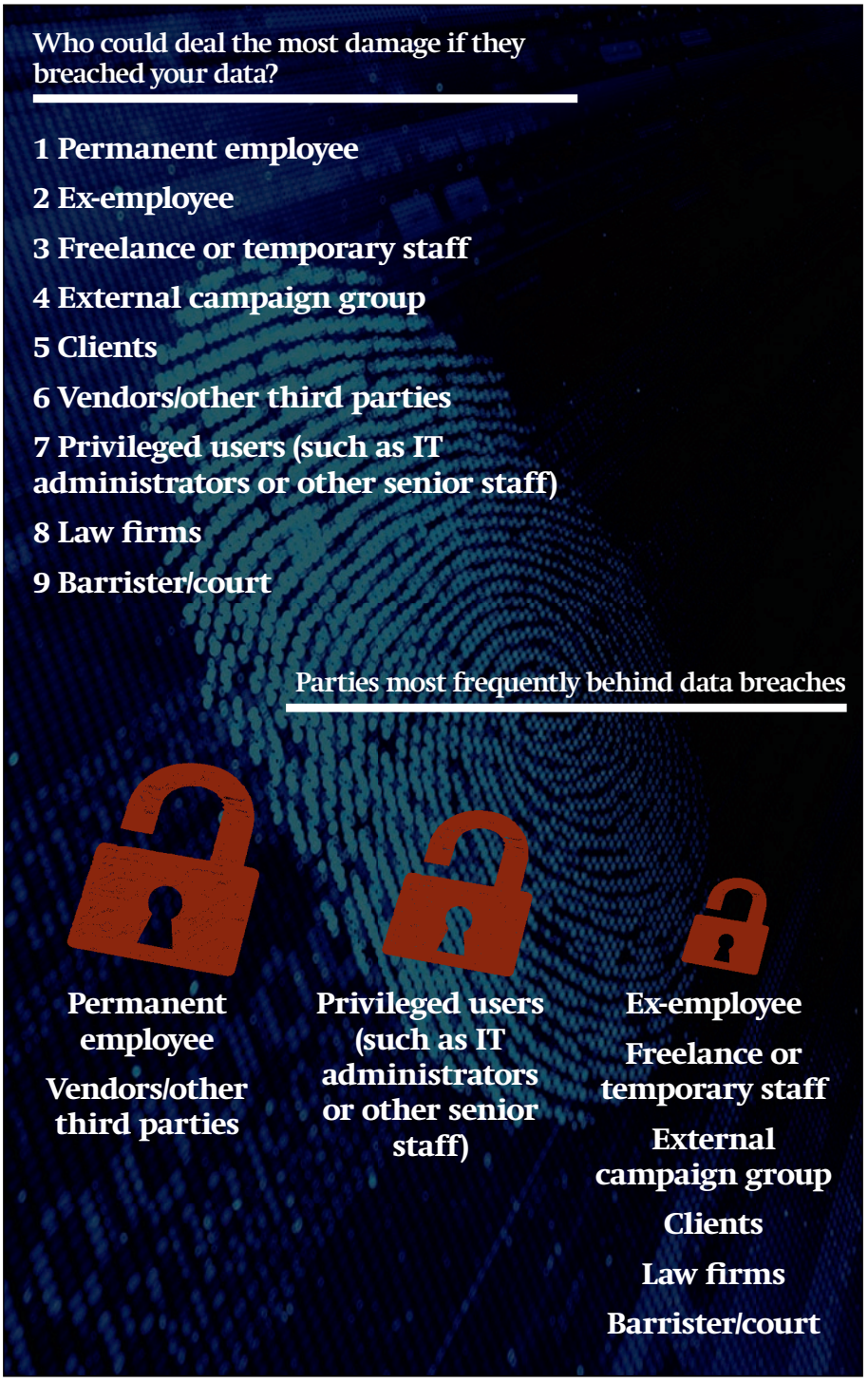
Knowing your data

The first measure is prioritisation. The wise business does not attempt to fight data battles on all fronts; that leads to failure. Instead, it identifies its most important data and defends this as best it can. In this way, it can deploy its finite resources in the most efficient way.

It is not merely a matter of being discerning. Hamilton points out that: "Companies need to know where their data is both physically and on IT systems and who has access to it.

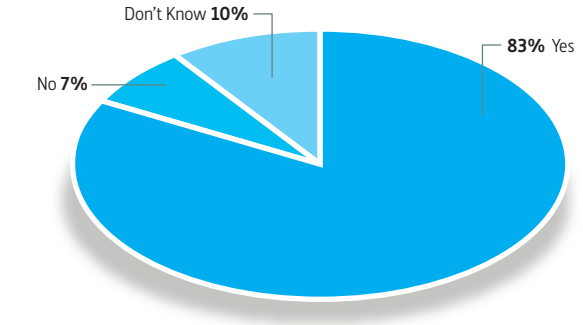
"If they do that, then that's brilliant. But I'm suspicious of those who say they do. We have a rather jaundiced view of those who claim to know all about their data and the access to it. They often in reality do not."

Legal Week Intelligence's survey found that while 88% of respondents were sure their company knew which of its data was the most important, 17% of this group did not know where this data was physically stored.

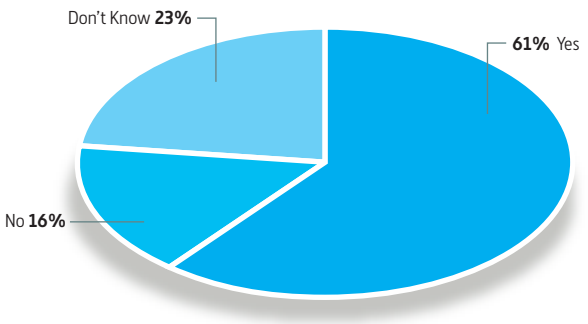


Data security supplement

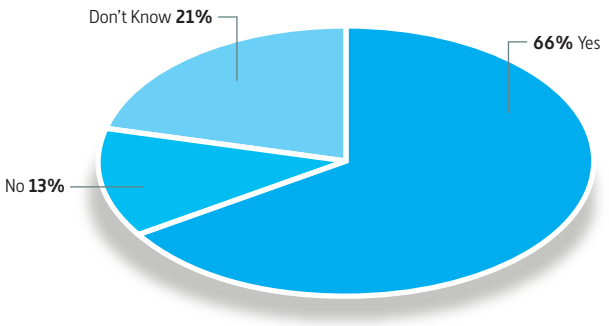
Does your organisation include terms in its contracts, detailing procedures to be followed in the event of a data breach?



If so, do you contractually require third parties who host data for your organisation to maintain a log of all events?



Do you require third parties to allow you to inspect their systems in the event of a suspected breach?



Monitoring access

Moreover, 30% of those businesses claiming to know what their most important data is either do not afford it the highest level of security or are unsure if they do, raising questions over who might be able to access it.

Kroll investigators frequently find that companies think data is secure but outsiders turn out to have access to it, quite legitimately in the case of suppliers or hosts of data.

"Any company is going to have confidential information and there should be controls on who can access it," Hamilton says. "If mergers and acquisitions policy, or employee bonus plans or quarterly results become public before official publication that can be disastrous because that information is extremely confidential."

Raymond agrees that this is a major factor in causing problems, and indeed has an example himself. "I was once in a job where I legitimately needed access to all customer data and the ability to alter it," he recalls. "I then moved into compliance and discovered I had kept those rights, when in that new role I needed to see data but not to alter it.

"Therefore one of the first things I did was to remove those privileges from myself. I think people who work in large companies tend to accumulate access rights for various reasons but then keep them even when they move to a different role and no longer need them, and that gives a greater chance that something will go wrong inadvertently."

Education

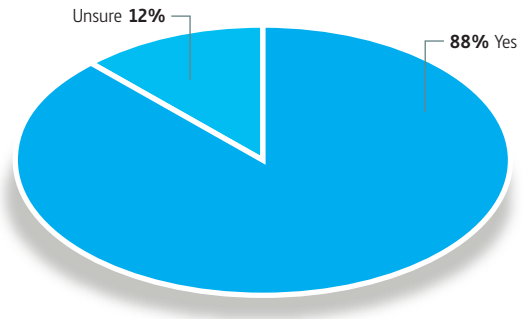
Changing hearts and minds is no less a factor in improving data security. Hamilton says defences installed against hacking "may be very good, but the hacker will bombard everyone in the company with an email with a link and when they click on it the hacker will gain access and can infect a system with malware very easily". Ensuring that staff know clearly what they may and may not do with a company's IT system, and why, is an essential part of the fight against such intrusions.

Relying on the judgement of employees may feel less comforting, to some, than the idea of enforcing a strict data security policy, but according to Zoe Newman, managing director of investigations and disputes at Kroll, security policies need to be pitched

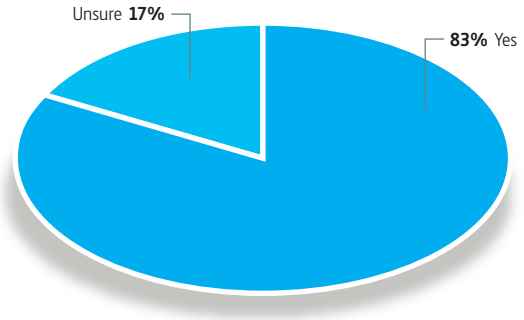
'People who work in large companies tend to accumulate access rights but then keep them even when they no longer need them, and that gives a greater chance that something will go wrong inadvertently'

Paul Raymond

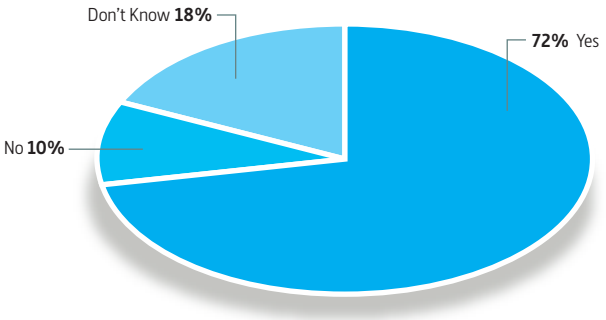
Does your organisation know what its most important data is?



If so, do you know where it is physically stored?



And is it more secure than other types of data?



‘We find that it’s only when people really understand why they are being asked to do something, that they change their behaviour’

Zoe Newman, Kroll

at the right level to change behaviour. “Too strict and they can be counter-productive as people don’t follow them; too permissive and they are not worth having. We find that it’s only when people really understand why they are being asked to do something, that they change their behaviour. Education is key.”

Flexible Working

The rise of bring your own device (BYOD) culture, and the attendant blurring of data borders, presents new dangers for corporate data security. James Watson, legal director of film and entertainment firm Deluxe, takes no chances. “We certainly don’t allow devices in areas where content is held or worked on — we operate to the highest industry standard as you would expect when our clients include Disney, Warner Brothers, Fox, Paramount, the BBC and ITV.”

However, to certain businesses, such stringency is not always possible, nor always desirable. Companies wishing to embrace more flexible working arrangements can gain a measure of protection through preventing staff from storing confidential data on their own tablets, laptops or mobile phones. After all, security on privately-owned devices will rarely match that on those owned by a company.

Third parties

Third parties can be “a problem, because it’s an unusual company that doesn’t use them for something, whether lawyers, public relations or whatever and they will sometimes legitimately have confidential data,” Hamilton says. “But do companies know what their suppliers’ controls will be like?”

Hamilton would not advise companies against storing any data on the cloud, but warns that using this can “introduce vulnerabilities unless you pick the right provider and are clear in your contract what is expected”.

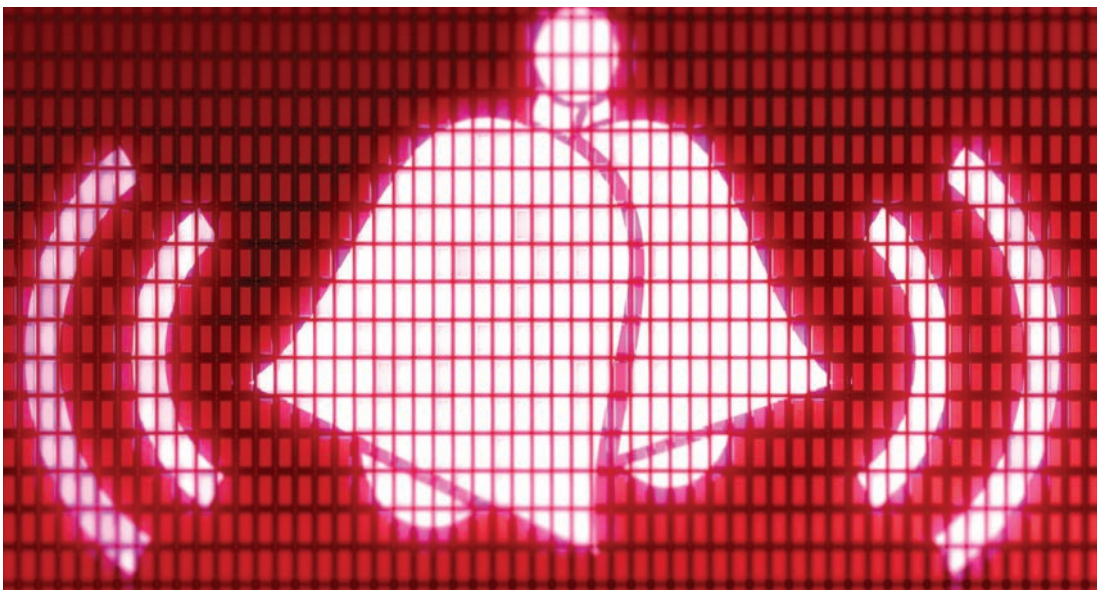
He adds: “It is little use if you need a record of who has accessed something and then find that recording that access was not specified in your original contract, so the provider never stored the information needed. When third parties have confidential data you need to be clear what can be done with it and what security they have.”

Detection

Prevention is better than cure, but when an attack does occur, speed and precision are of the essence.

Legal Week Intelligence’s study found, somewhat alarmingly, that, of those businesses which had suffered data breaches in the past 12 months, only a quarter could say how many such breaches had occurred, let alone been suspected.

Even among those who are aware enough to know that a breach has occurred, there clearly exists a profound blindness to the extent of the problem.



This chimes with another finding, which shows that only six in ten businesses require third parties hosting their data to maintain a log of all events. Similarly, only around two thirds of businesses reserve a right to inspect their third parties' systems in the event of a breach.

Such results raise serious doubts over how quickly businesses can detect breaches of their data, particularly given the likelihood of a breach by a vendor or other third party. It would seem that, where data is concerned, much trust — perhaps too much — is given on trust alone.

CONCLUSION

The survey findings suggest that most businesses are not as attuned to data security as they should be — or, indeed, they think they are. In order to guard themselves against damaging data breaches, these companies will need to change their approach to this important issue.

The image which businesses appear to have of their enemy needs to be urgently updated. Though external assailants do remain a problem, organisations need to recognise that most data breaches are committed by internal personnel, and that many instances of external threats in fact originate this way.

Similarly, hacktivists engender more concern amongst businesses than third party vendors and privileged users.

Yet the survey results also show that these latter parties are far more likely to cause a breach than external campaign groups alone.

In the vast majority of cases, data breaches reported by respondents were accidental rather than deliberate.

Given that internal agents play such a large role in committing such breaches, this suggests the existence of a large blind spot within corporate data management; one which could be remedied with better education, tighter security policies and more vigilant monitoring.

Such remedies are by no means easy to effect, particularly in the age of flexible working. However, by teaching employees to spot the key attack vectors and incentivising them to adopt best practice procedures, gaps in the fence can be minimised.

Above all, the key is to identify what one's most important data is, and to concentrate efforts on safeguarding it.

Case study

Information leak: Investigation on behalf of a listed UK financial institution

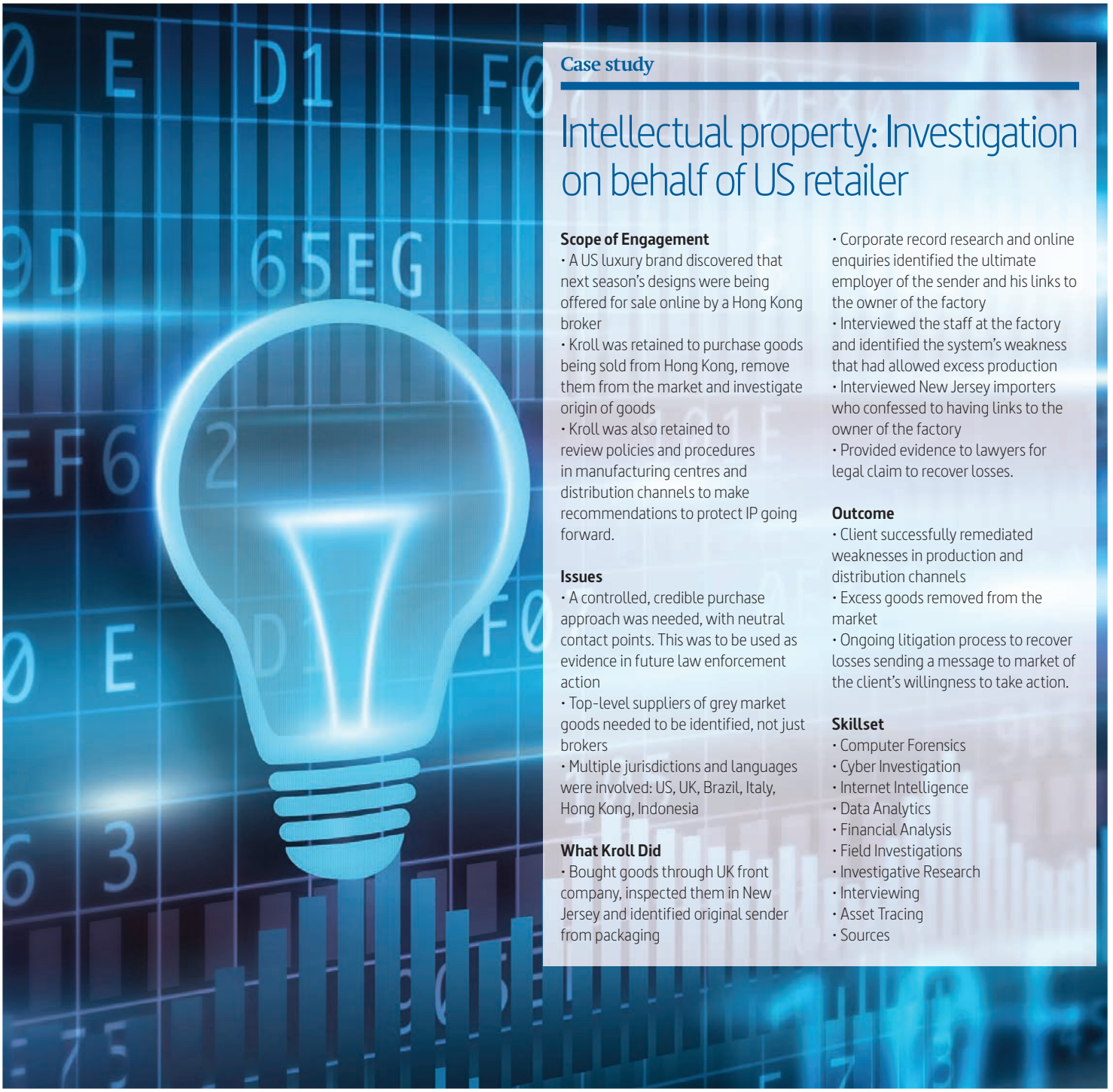
Scope of Engagement
- Kroll was retained to investigate the leak of board level information to the media that resulted in share price fluctuation
- Kroll was asked to report to the chairman and non-executive directors, with a copy to regulators

Issues
- Confidentiality — the issue was still "live" and was the subject of ongoing publicity in national press
- Privacy — personal telephones and communications equipment were relevant to the investigation
- Sensitivity — seniority of people being questioned about their integrity
- Urgency — board wished to be seen to make appropriate response

What Kroll Did
- Persuaded all relevant individuals to allow Kroll to image their personal and corporate phones, and access emails, to enable a full chronology of the relevant time period
- Forensic mapping of the evolving circle of knowledge of the key facts
- Identified errors in the journalist's state of knowledge and cross referenced them to the state of knowledge of individuals in the institution
- Careful and subtle interviewing of the relevant individuals in the institution
- Reported conclusions orally to board committee and then provided written report

Outcome
- Identification of the two people responsible for the leak through their own inconsistencies and common errors with the journalist
- Board member responsible left the business by mutual agreement
- Regulators satisfied that appropriate steps had been taken
- No further board level leaks from organisation to date

Skillset
- Computer Forensics
- Internet Intelligence
- Data Analytics
- Investigative Research
- Interviewing



Case study

Intellectual property: Investigation on behalf of US retailer

Scope of Engagement
- A US luxury brand discovered that next season's designs were being offered for sale online by a Hong Kong broker
- Kroll was retained to purchase goods being sold from Hong Kong, remove them from the market and investigate origin of goods
- Kroll was also retained to review policies and procedures in manufacturing centres and distribution channels to make recommendations to protect IP going forward.

Issues
- A controlled, credible purchase approach was needed, with neutral contact points. This was to be used as evidence in future law enforcement action
- Top-level suppliers of grey market goods needed to be identified, not just brokers
- Multiple jurisdictions and languages were involved: US, UK, Brazil, Italy, Hong Kong, Indonesia

What Kroll Did
- Bought goods through UK front company, inspected them in New Jersey and identified original sender from packaging
- Corporate record research and online enquiries identified the ultimate employer of the sender and his links to the owner of the factory
- Interviewed the staff at the factory and identified the system's weakness that had allowed excess production
- Interviewed New Jersey importers who confessed to having links to the owner of the factory
- Provided evidence to lawyers for legal claim to recover losses.

Outcome
- Client successfully remediated weaknesses in production and distribution channels
- Excess goods removed from the market
- Ongoing litigation process to recover losses sending a message to market of the client's willingness to take action.

Skillset
- Computer Forensics
- Cyber Investigation
- Internet Intelligence
- Data Analytics
- Financial Analysis
- Field Investigations
- Investigative Research
- Interviewing
- Asset Tracing
- Sources

Case study

Cyber: Middle East energy supplier

Scope of Engagement
- Client suffered significant data breach and damage to systems by external hackers who had been inside company systems for three months
- Kroll was engaged to provide investigations expertise and to determine the scale and nature of what had happened, who had done it, and to examine the roles of employees
- Kroll was retained by US counsel to maintain legal privilege and confidentiality over findings

Issues
- Confidentiality – there was extensive coverage of the event in the media
- Data protection – the investigation could not take information out of the host nation without government approval
- Cultural issues around working in the Middle East, including different sensitivities during interviews
- Political issues arising from the possible involvement of another nation state

What Kroll Did
- Rapid response
- Won court orders in France to disclose ownership details of key server used in exfiltration
- Analysed vast amounts of data to obtain a patchwork of clues that identified the perpetrators, and then profiled their international and domestic footprints for law enforcement
- Clarified the errors and omissions by employees that enabled the breach and recommended changes to procedures and architecture to prevent a recurrence
- Provided report to local prosecutor to explain why Kroll did not believe there had been an insider involved

Outcome
- Client confident that it understood what had happened and by whom
- Client was able to reassure government that the problem had been dealt with appropriately and lessons learned
- New procedures instituted by the client to enhance controls and provide a layered defence against attacks

Skillset
- Computer Forensics
- Cyber Investigation
- Internet Intelligence
- Data Analytics
- Field Investigations
- Investigative Research
- Interviewing
- Sources

Kroll®

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.

FRAUD	BRIBERY AND CORRUPTION	FORENSIC ACCOUNTING	ASSET TRACING AND RECOVERY
LITIGATION SUPPORT	DISPUTE RESOLUTION	TRANSACTION INTELLIGENCE	INFORMATION SECURITY AND CYBER THREATS

Please contact us for more information:

krolluk@kroll.com | +44 (0) 20 7029.5000

kroll.com