ALLEN & OVERY

The Big Think

Cybersecurity – the threat from within

September 2016

allenovery.com

“Cybersecurity is not just some kind of buzz word for our clients any more. It’s a top priority for boards because it’s increasingly obvious that everyone is vulnerable in so many ever-changing ways.”

Sarah Henchoz, Partner (London)

Contents

Jargon buster – cybersecurity terminology*

Botnet – A collection of computers subject to control by an outside party, usually without the knowledge of the owners, using secretly installed software robots.

Cybersecurity – Measures taken to protect computers or critical infrastructure.

Denial-of-service attack – Flooding the networks or servers of individuals or organisations with false data requests so they are unable to respond to requests from legitimate users.

Hacker – A person with special expertise in computer systems and software. A hacker who attempts to gain unauthorised access to computer systems is a "cracker".

Hacktivist – An individual who breaches websites or secured communications systems to deliver political messages, including those related to foreign policy, or propaganda.

Malware – Any code that can be used to attack a computer by spreading viruses, crashing networks, gathering intelligence, corrupting data, distributing misinformation and interfering with normal operations.

Pharming – The act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Phishing – Using a fake email to trick individuals into revealing personal information, such as Social Security numbers, debit and credit card account numbers and passwords, for nefarious uses.

Spam – Unsolicited bulk email that may contain malicious software. Spam is now said to account for around 81% of all email traffic.

Spear Phishing – A type of phishing attack that focuses on a single user or department within an organisation, addressed from someone within the company in a position of trust and requesting information such as login IDs and passwords.

Spoofing – Making a message or transaction appear to come from a source other than the originator.

Spyware – Software that collects information without a user's knowledge and transfers it to a third party.

Trojan horse – A destructive program that masquerades as a benign application.

Virus – A program designed to degrade service, cause inexplicable symptoms or damage networks.

Worm – Program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down. A worm, unlike a virus, has the capability to travel without human action and does not need to be attached to another file or program.

*Source: Homeland Security

About this report

Few risks have risen so quickly up the boardroom agenda as cybersecurity.

Just a distant concern a few years ago, it is now routinely regarded as being among the top risks faced by companies, large and small. And all the stats suggest that the problem is growing, with more and more firms suffering increasingly expensive security breaches.

More worryingly, the risk is coming from all directions and not just from lone wolf hackers, organised criminal gangs or shadowy state-sponsored agencies mounting increasingly sophisticated external attacks – though these threats are all real.

In fact, the highest proportion of breaches these days emanate from inside organisations. It could be the work of a disgruntled employee or an industrial spy. But, more likely, it will be the result of simple human error – a lost laptop or a careless click on a cleverly disguised email attachment that immediately opens the door to an attacker.

Cybersecurity throws up a whole host of complex issues for risk managers to plan for and mitigate – technological, reputational, legal and cultural.

But, in this, Allen & Overy's fifth Big Think publication, we focus on the employment aspects and ask: what can employers do to build truly secure cyber defences? Are they putting the right resources into training and educating their workforces or relying too much on technology to thwart attacks? Is it possible to pre-screen potential recruits or monitor the activity of existing employees without falling foul of fast-changing privacy and data protection laws? What policies and contractual obligations can be legitimately placed on workers? How can companies plan for the public firestorm unleashed when employee or customer data is compromised?

Cyber insecurity – a growing scourge

Advances in technology, much greater connectivity and the ability to store and analyse huge quantities of data are all offering companies new and efficient ways to organise themselves and extend their reach to new markets and customers.

But with these opportunities come risks and none is more alarming than the constant and growing threat of highly sophisticated cyber attacks.

In a relatively short time this threat has grown to become one of the most significant risks faced by companies across sectors – a risk that is evolving at such high speed that it is very hard to control and mitigate.

In fact, it's said that there are only two types of company where cybersecurity is concerned – those that have been hacked and those that have been hacked, but don't yet realise it.

If that claim sounds exaggerated, think on.

There is a growing body of evidence to suggest that few organisations, no matter how large or small, are immune from serious breaches in security.

The numbers

That's certainly the picture painted by the UK government's latest statistics.

According to the UK Information Security Breaches Survey 2015, conducted for the government by consultants PwC, a staggering 90% of large organisations suffered a security breach during the year – up from 81% in 2014. For small companies, the figure was lower but growing even more quickly – up from 60% in 2014 to 74% last year.

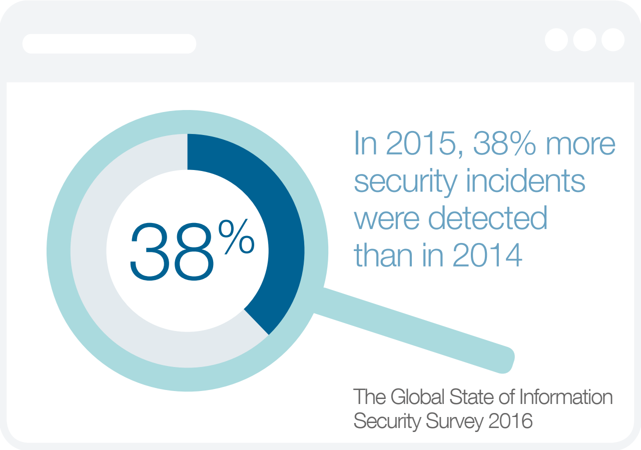
What's more, the cost of these breaches continued to soar, with the average cost for a large company put at between GBP1.46 million and GBP3.14m and at between GBP75,000 and GBP311,000 for smaller business. In both cases, this represents a doubling of the costs reported in 2014 and amounts to the sort of significant financial hit that few enterprises can afford to bear.

Internationally the picture is very similar. PwC's Global State of Information Security Survey 2016, based on responses from some 10,000 executives in more than 127 countries, found that there were 38% more security incidents in 2015 than in the previous year. There was also an alarming growth in the theft of hard intellectual property up by 58% in 2015.

While this survey found that the average financial loss due to security breaches fell very slightly in 2015, the amount of money being spent by companies on bolstering their information security rose by a substantial 24%.

This alarming picture is confirmed by the work we are doing with clients on all aspects of cybersecurity across regions – whether that is advising them on how to deploy sophisticated IT defence tools, helping them to monitor activity within their operations while still complying with differing data protection and privacy laws, working with them to plan for and crisis-manage a security breach, or offering guidance on how to train and educate their staff to be "cyber safe".

Indeed, the general counsels and executives we are working with now typically cite cybersecurity as one of the top three issues on their boardroom agendas.



In 2015, 38% more security incidents were detected than in 2014

The Global State of Information Security Survey 2016

Theft of 'hard' intellectual property increased by 56% in 2015

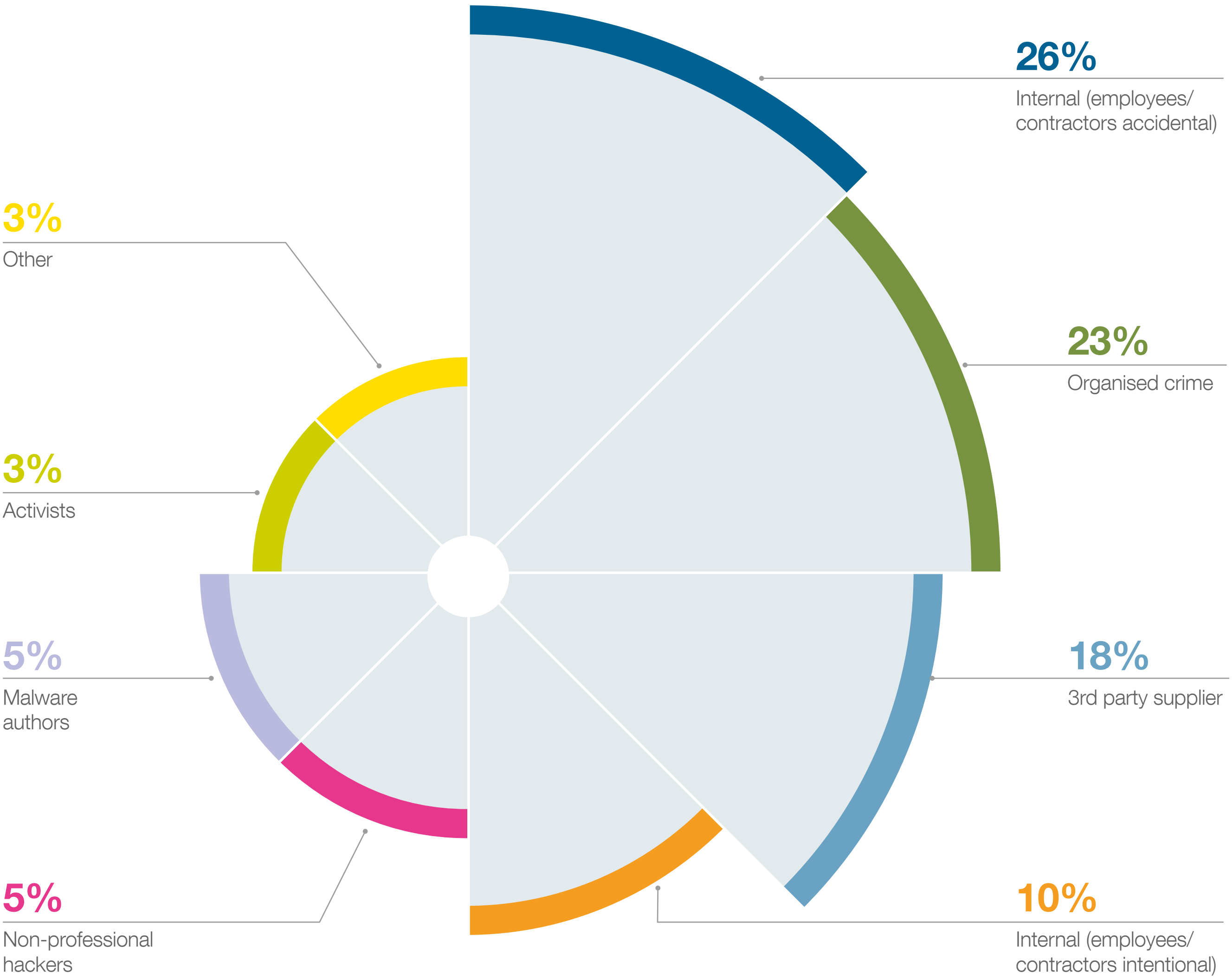
The Global State of Information Security Survey 2016

That's not surprising. Awareness of the risk is rising rapidly, thanks to a continuing stream of high-profile cases where sensitive information has been accessed, stolen, held for ransom or leaked, with painful legal, financial and reputational damage done to the companies or individuals involved.

The giant Sony attack in 2014 – variously blamed on North Korea, hackers and company insiders – was so huge in scale that it served as a massive wake-up call to many companies. The hack of personal data from Ashley Madison, the website set up for people seeking extra-marital affairs, underlined the sheer scale of data that can be involved, with the personal details of 33 million user accounts published online.

Last year's attack on the UK telecoms company Talk Talk saw details of 157,000 customers accessed and 15,600 bank account numbers and sort codes stolen by hackers. And this year's global media coverage has been dominated by the leak of the so-called "Panama Papers" with exposé after explosive exposé of the tax evasion techniques used by some of the world's wealthiest and most powerful people.

What was the origin of the threat/source of the breach?



UK Information Security Breaches Survey 2015

The threat from within

But these are the headline-grabbing cases, and to some extent they mask both the hour-by-hour challenge that many companies face and where the biggest threat is coming from.

In reality, the biggest problem lies within organisations, no matter how strong their external cyber defences – the risk that an employee, either by accident or intent, causes a serious breach of security from the inside.

Again the UK government's statistics throw this reality into stark relief. Its survey found that – although 26% of breaches in 2015 were caused by organised crime and a further 5% were from non-professional hackers – an astonishing 36% of breaches were caused by employees or contractors.

Of those 10% were intentional – the work, perhaps, of a disgruntled employee or an industrial spy downloading valuable data onto a phone or a USB stick.

The rest (26%) were accidental; simple acts of human error.

And when asked to identify the cause behind the biggest breach suffered by their organisation, half of all survey respondents put it down to human error.

Once again this is reflected internationally. PwC's latest global report found that present and past employees remained the biggest source of compromises to security, at 34% and 29% respectively. But the fastest growing source of incidents was contractors and other business partners – up from 18% in 2014 to 22% in 2015.

Although there are many ways an internal security breach can occur, one is becoming increasingly familiar.

An external attacker hides a virus or piece of malware in an attachment to an innocent-looking email. It looks like it comes from a reliable source – a government department, perhaps, or a household-name company.

Sometimes the email may be scattered indiscriminately around an organisation in the hope someone will take the bait. Or it may target an individual within the company or down the supply chain. The hacker may even use social media to track that individual's interests and pastimes, and approach with an enticing and entirely plausible personalised offer – free tickets to a big sporting event, this week's menu from a favourite restaurant, a change of time for the delivery of an online supermarket shop.

In an unguarded moment, the employee forgets all the warnings about cyber subterfuge and the need to send suspicious communications straight to the IT team for checking. He or she opens the email, clicks quickly on the link – and the attacker is in.

Sarah Henchoz, a partner in our London office, has seen a marked change in how clients across sectors are reacting to this threat: "Cybersecurity is not just some kind of buzz word for our clients any more. It's a top priority for boards because it's increasingly obvious that everyone is vulnerable in so many ever-changing ways.

"And it's also become clear that employees are a crucial part of this story – potentially both a company's biggest asset in guarding against threats, but also its most obvious vulnerability. With the right approach – backed by the right blend of education, training, policies, practices and reporting procedures – they can become the strongest line of defence against attack."

Tobias Neufeld, a partner in our Düsseldorf office specialising in employment law and data protection, notes that many companies are relying on technology – new patches, new apps – to screen for and protect against external threats.

"That's obviously the right approach in some respects – attackers can be foiled by technical defence mechanisms and it's important that companies continuously update their defences to meet the evolving threat," he says.

"But I'm surprised that using technology is often their first response. The evidence is clear that most breaches are down to human error – employees not closing down their PCs properly, losing laptops or smartphones, sending confidential information via private email, using weak passwords and codes, clicking on that email link. Companies need to recognise that human error is still the number one threat they face."

> *"I'm surprised that using technology is often their first response. The evidence is clear that most breaches are down to human error."*

Tobias Neufeld, Partner (Germany)

GBP36,500

average cost of a breach to large business

Cyber Security Breaches Survey, 2016

Ahmed Baladi, a partner in our Paris office, notes that there are three types of company when it comes to dealing with cyber threats.

There are relatively mature companies – often, large, multinationals – with powerful in-house IT security teams who are increasingly protecting themselves effectively against external attack.

Then there are smaller companies relying on third party IT suppliers who wrongly assume that responsibility for cybersecurity has been contracted out and is not their concern.

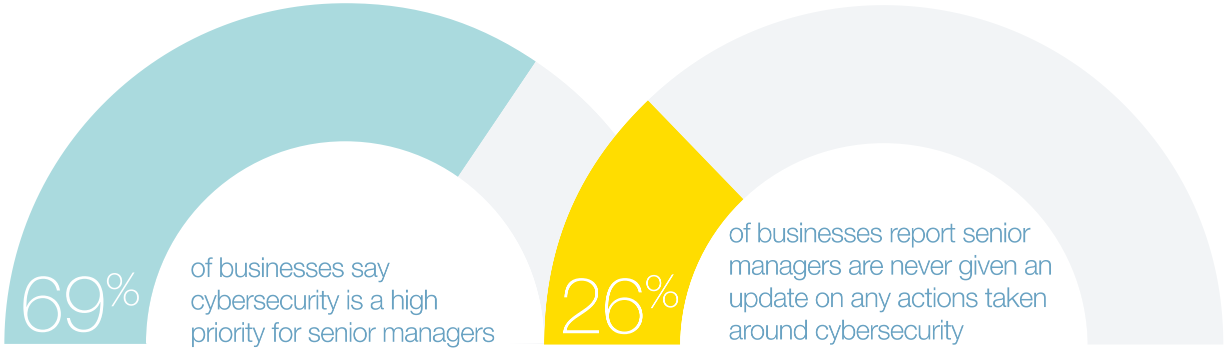
And finally there are a whole range of small businesses who remain "completely negligent" about the issue – a group, he says, that is gradually getting smaller as awareness grows.

But in all three cases, educating and training employees to be more cyber secure in their everyday working practices remains a surprisingly low priority.

"Many companies, including those who are most advanced in dealing with threats, have a basic misconception about cybersecurity. They think the main threat is coming from some anonymous activist in a remote country designing increasingly intricate ways to break into IT systems to steal data.

"There's only so much you can do about an external attack, but masses you can do to tackle the threat from within the organisation – that's the risk you really need to address."

Sheila Fahy, professional support lawyer counsel in the London employment practice, agrees: "There is no doubt that cybersecurity is one of the top priorities for companies. Initially the focus was on taking steps to prevent external attacks, but now the focus has shifted to the threat from within, and to educating employees to be the first line of defence."



69% of businesses say cybersecurity is a high priority for senior managers

26% of businesses report senior managers are never given an update on any actions taken around cybersecurity

Cyber Security Breaches Survey, 2016

Regional scan – a changing legal landscape

The need to improve levels of security has been heavily underlined by changes in the law, not least in Europe.

Ahmed Baladi notes that, in the past, many companies tried hard to keep any security breaches they had suffered under wraps, concerned about the high financial and reputational costs they might incur if a breach made front-page news.

But that is changing now with the advent of two new pieces of EU regulation forcing companies to report security breaches immediately to national authorities (see more Cybersecurity legislation on page 24 for a list of new and promised data regulation). These are likely to affect UK companies too, regardless of Brexit, as EU laws will apply in the UK until the point that it leaves. And it is likely to be a condition of any future EU trading deal that the UK implements similar standards.

> *"In general when you consider all of the disparate Federal and State laws the reality for a multinational company is that, if you are compliant with all UK and European laws, you are likely to also be compliant in the U.S"*
>
> Brian Jebb, Senior Counsel (U.S.)

The new EU legislation is, in one sense, very welcome, says Inge Vanderreken, a partner in our Brussels office. "To some extent it harmonises a lot of data protection rules across the EU making it easier for companies operating across borders. But it is important to remember that different national laws operate in this area and companies need to be sure they are compliant."

In general, U.S. and UK data processing and privacy regulation is much more permissive. That's problematic for multinational companies, says Sarah Henchoz. "What you may be able to do in the UK is very different to what you can do in, say, Germany, and that can cause real challenges. Managing an increasingly flexible and mobile workforce is also an issue. Companies need to be clear where their data is located and how it is being used," she says.

That's because in northern European countries, including Germany, the Netherlands, Belgium and France, restrictions on processing employee information and privacy remain very strict often for deeply rooted cultural reasons. "If you look at Germany's history since World War II, you can easily understand why we are very sensitive about this issue," says Tobias Neufeld.

By contrast, a decree issued last year under Italy's new Jobs Act has significantly loosened rules on monitoring employees in the workplace for the first time since the 1970s, according to Livio Bossotto, head of our Italian employment and benefits team. The consensus is that the new law also covers checking up on the use of company-issued IT tools.

The U.S. has no single data processing regime. Instead it has what Brian Jebb, a Counsel in our New York office, describes as "a hotch-potch of Federal and State laws which tend to focus on specific subjects or sectors".

"In general when you consider all of the disparate Federal and State laws the reality for a multinational company is that, if you are compliant with all UK and European laws, you are likely to also be compliant in the U.S. – our laws aren't generally as onerous and our protections are not as comprehensive," says Brian. "The problem often arises the other way, for U.S. companies looking to operate across borders in Europe."

Data processing legislation is also considerably less developed in China and Hong Kong, although the latter has had regulation in this area since the mid-1990s, an active data protection authority willing to pursue breaches of its guidelines, and has now established a special cybersecurity and technology crime taskforce, according to Susana Ng, a consultant in our Asia Pacific regulatory team.

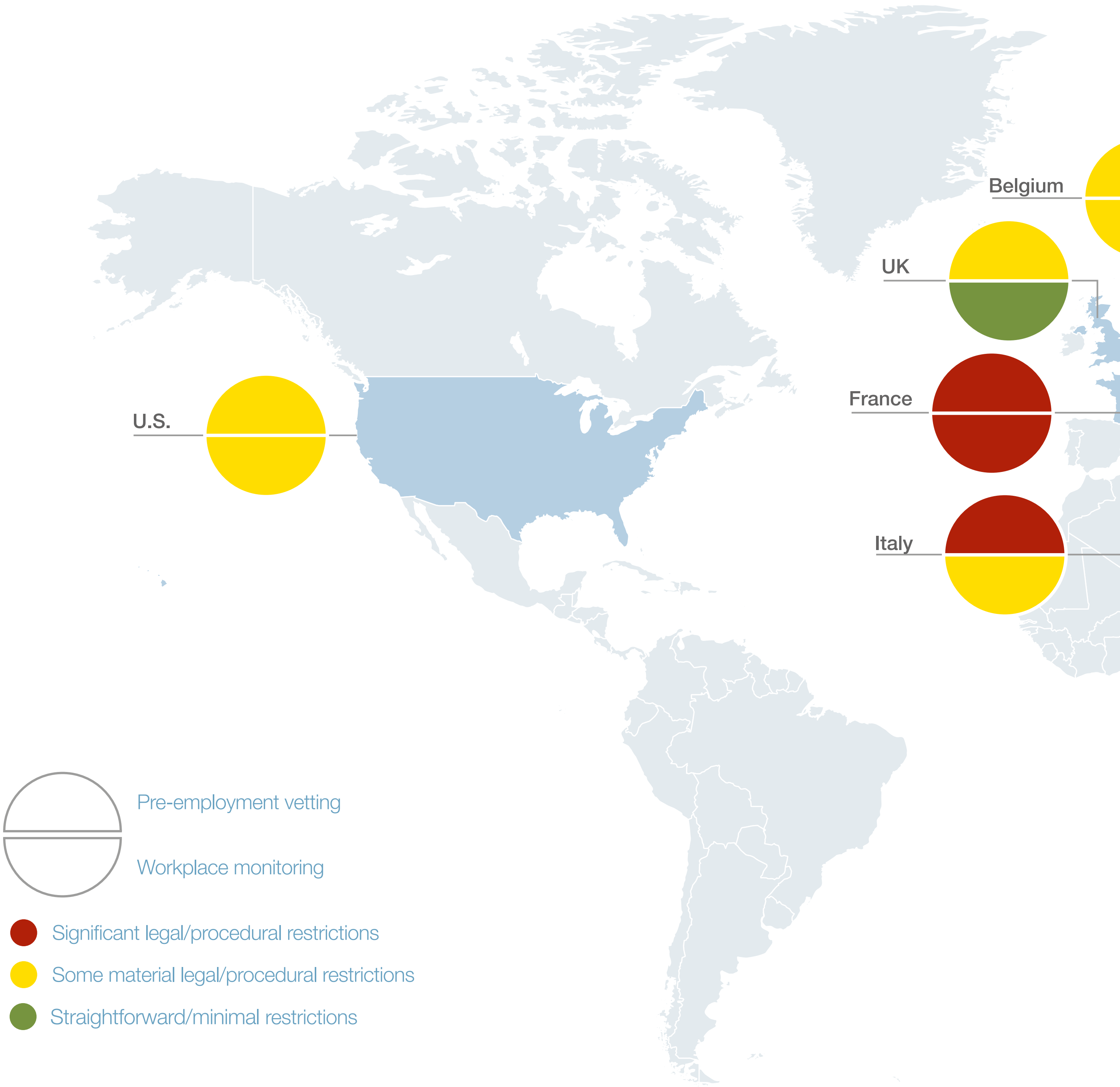
The Chinese government has also drawn up draft cybersecurity legislation signalling that this is a top priority for the PRC government.

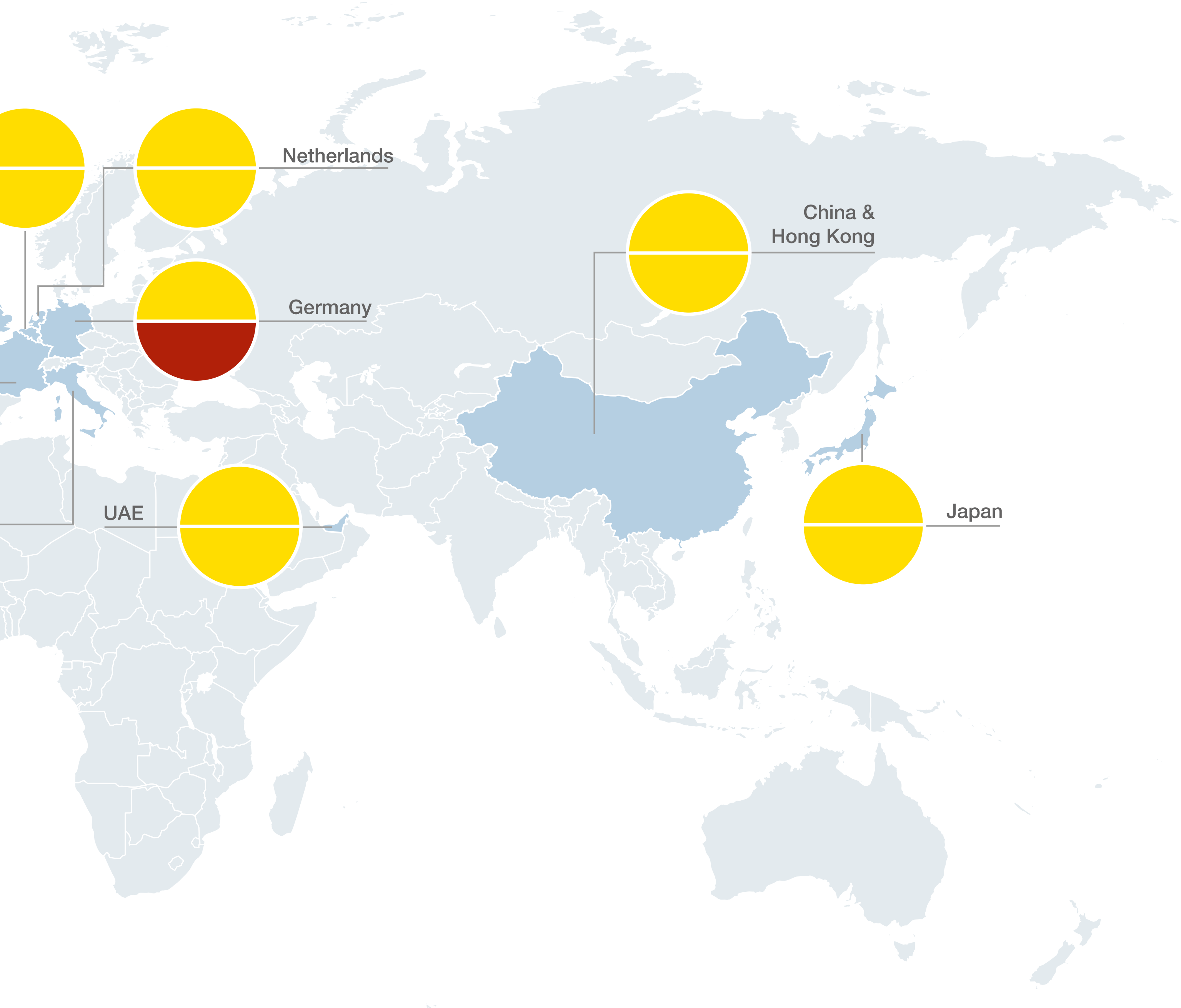
One significant issue for multinational companies operating here concern the guidelines already in place restricting the transfer of information out of China, but no data protection regime, and no one agency, enforcing it. For companies used to much clearer rules and structures in Europe or even the U.S., this is creating uncertainty in an important marketplace, Susana says.

Broadly drawn national security laws also present particular problems for inbound investors forming joint ventures with Chinese state-owned enterprises. "It raises questions about whether overseas transfer of the information divulged by the Chinese partner constitutes a breach of national security – for which there are criminal sanctions," Susana continues, "It also means that a multinational may not be able to transfer important commercial information back to its headquarters."

That is a problem in other emerging markets as well, not least India and Russia, adding cost and complexity for companies operating across borders.

Legal restrictions on pre-employment vetting and workplace monitoring


Belgium
UK
U.S.
France
Italy
Pre-employment vetting
Workplace monitoring
Significant legal/procedural restrictions
Some material legal/procedural restrictions
Straightforward/minimal restrictions


Netherlands
China &
Hong Kong
Germany
UAE
Japan

Cyber safe – keeping your own house in order

Preventing highly sophisticated attacks from outside the organisation will, as we have said, always be a challenge.

But there is a surprisingly long list of actions a company can take from an employment perspective – practical, technological and contractual – to limit and mitigate the risk of inadvertent internal security breaches.

> *"There are some great training materials on the market that bring cybersecurity to life and underline the fact that employees share the responsibility for staying cyber safe"*
>
> Shelia Fahy, PSL Counsel (London)

Education and training are essential

Consistent and regular education and training must be central to the security strategy, not least because it is the best way to ensure that awareness of the threat remains high at all times. Organisations should make it an essential part of the induction process for new employees and ensure that training is repeated and updated at regular intervals, including information about the latest scams.

And it is a very effective way to bring about necessary cultural change. There is a tendency in some companies for employees to think that responsibility for cybersecurity lies with the chief information security officer and the IT team. In truth, the most secure companies are those where employees understand that cybersecurity is the responsibility of every individual in the organisation.

"There are some great training materials on the market that bring cybersecurity to life and underline the fact that employees share the responsibility for staying cyber safe," says Sheila Fahy. It is important to include specifics such as vulnerable hot spots like social networks and fraudulent attempts to extract critical data like passwords. "This doesn't need to be a hard sell. Employees own computers and smart devices at home, so are likely to see such training as being of great personal value."

Sander Schouten, senior associate in our Amsterdam office, says companies should use all the awareness raising techniques used by other institutions, like banks and retailers, to constantly warn of the threats – videos and pop-up warnings on the computer system, for instance.

"There's a lot of focus on restrictive governance in companies – rules and procedures – but my feeling is that the real problem lies internally with the threat of inadvertent breaches and that's really all about education and awareness," he says.

> *"There's a lot of focus on restrictive governance in companies – rules and procedures – but my feeling is that the real problem lies internally with the threat of inadvertent breaches and that's really all about education and awareness"*

Sander Schouten, Senior Associate (Netherlands)

The role of company policies

Policies – on such things as the proper and safe use of IT, internet usage, email protocols and the use of mobile devices, whether company-owned or personal – do, of course, have a very important place in the cybersecurity armoury.

It's important that these policies tie in closely with training programmes and that they link together in a consistent way.

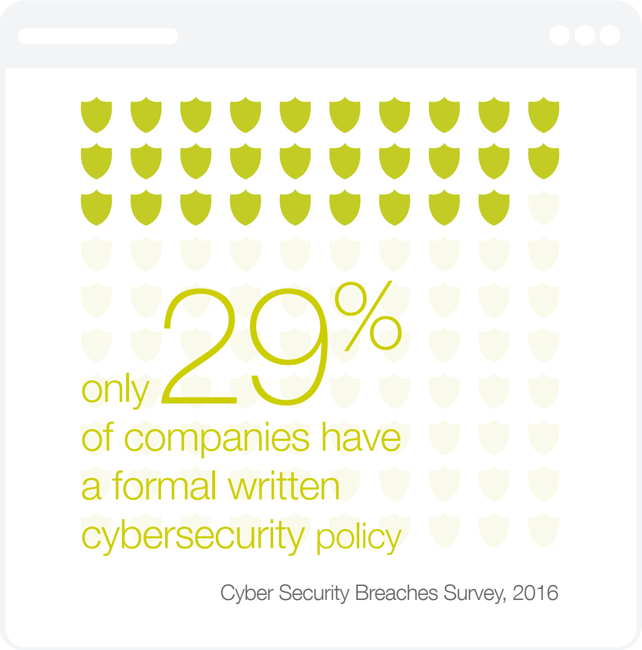
Above all it's essential that they are always clear and transparent so that employees fully understand their responsibilities and obligations and what sanctions will be used when they do not comply. They should also encourage employees to report incidents and concerns.

As more and more companies encourage their employees to bring their own devices to work and use them for work-related tasks, this is an area where very clear policies and guidelines are needed. Employers have much less control over these devices than tools provided by the company.

Mobile technology is a point of particular vulnerability. It is an ideal vehicle for importing malware into an IT infrastructure and an easy way to export valuable data – gone are the days when a disgruntled employee or industrial spy needed to heave a sackful of sensitive documents out of the building. These days it can be quickly loaded onto a mobile device and quietly pocketed.

Bring Your Own Device (BYOD) policies will differ from organisation to organisation. But there are some common features that most companies can adopt – spelling out what security settings are required, for example, how confidential data should be stored, on what grounds it can be transferred and how the data will be recovered if the employee quits or if the device is lost or stolen.

In the case of lost or stolen devices, some effective technological solutions are available. Companies can, for instance, register personal devices to a remote "locate and wipe" facility allowing data to be remotely deleted on demand.



only 29% of companies have a formal written cybersecurity policy

Cyber Security Breaches Survey, 2016

Contractual obligations – watch out for cultural differences

Company policies and procedures can, in some circumstances, be significantly bolstered by placing specific contractual duties and obligations on individual employees.

Employees often owe a duty to their employer under the common law – whether that be a duty of mutual trust and confidence or a duty of confidentiality. But these can be strengthened, in some jurisdictions, with the inclusion of express clauses in contracts and service agreements.

Some of our clients, for instance, include specific confidentiality clauses in contracts, as well as specific duties to disclose wrongdoing and to comply with company policies. We even see that being extended to employees leaving the company, with the inclusion of restrictive covenants and "garden leave" clauses to place restrictions on staff in the immediate post-employment phase.

But this is not common practice in all jurisdictions. As Sander Schouten points out, Dutch employers tend to rely on the accepted code of "good employeeship" and general whistle-blowing policies to encourage employees to report wrongdoing. Specific contractual obligations are not seen in the Netherlands, he says.

Employment contracts in Italy tend to be relatively simple and make reference to the general collective agreement, where one exists, says Livio Bossotto. They may contain references to confidentiality and non-compete clauses, but rarely cover the reporting of wrongdoing.

Indeed, Italian companies are still obliged to display codes of conduct in accessible places in their workplaces to spell out policies and detail possible sanctions. "It's an old rule from the 1970s which, despite huge changes in the workplace, continues to be enforced," he says. But he notes that, with the liberalisation of employee monitoring rules and a new policy on whistle-blowing promised by the Italian government, there could be significant changes in the coming months and years.

Getting contracts right becomes increasingly important for senior management roles, and it's important that general fiduciary duties are clearly set out in director and senior level contracts.

In some jurisdictions these fiduciary duties are now being enforced with growing rigour, not least in Germany where board directors of private limited companies have a duty to manage risk to a very high level, including setting up an effective and safe IT infrastructure.

This, says Tobias Neufeld, has been enforced increasingly strictly following the bribery scandal at Siemens in 2006, focusing on its former CFO Heinz-Joachim Neubürger. "Since the Neubürger case, there is now a general strict obligation on all directors to set up a proper organisation with respect to governance and compliance," he says.

> *"Employment contracts in Italy tend to be relatively simple and make reference to the general collective agreement, where one exist. They may contain references to confidentiality and non-compete clauses, but rarely cover the reporting of wrongdoing."*
>
> Livio Bossotto, Counsel (Italy)

Proportionate pre-employment checks

How far a company can go in running pre-employment checks on a potential recruit varies quite radically from jurisdiction to jurisdiction. Employers have considerably greater scope to do pre-screening in the UK and the U.S. than in continental European countries.

Some companies in IP-rich or strategic sectors, such as life sciences, finance, energy, transport and defence, are increasingly keen to run such checks and some have even asked if they might get access to government watch lists when hiring for particularly sensitive roles.

Yet, even in the UK, data protection rules only allow vetting where there are particular risks and where there are no less intrusive alternatives. The Information Commissioner's Office has, for instance, issued an Employment Practice Code which advises against comprehensive screening other than in exceptional cases.

The accent, even in this more liberal regime, is on using vetting in a proportionate and non-discriminatory way. And even those employers running social media checks on potential recruits need to be balanced in their approach – they should inform candidates and be careful not to place too much reliance on what they find without giving the applicant the chance to make representations.

> *"There's a big difference in what's possible with pre-employment vetting in continental Europe than in the UK and U.S. where there is more flexibility and greater access to databases."*
>
> Inge Vanderreken, Partner (Belgium)

Restrictions on pre-employment screening are invariably much stricter in other parts of Europe.

As Inge Vanderreken puts it: "There's a big difference in what's possible in continental Europe than in the UK and U.S. where there is more flexibility and greater access to databases," she says.

"In Belgium – although 80% of companies in a recent survey said they did some kind of pre-employment screening – they, or third party agents working for them, are limited to publicly available data only. Therefore, in order to receive more detailed information on the candidate, they need the candidate's consent and cooperation. Indeed, access to criminal records or other certificates is forbidden by anyone other than the individual involved." In the Netherlands employers are allowed to seek "certificates of good conduct" from designated government departments but these are always job specific – a car accident history for someone applying to be a taxi driver, for instance – and only the candidates themselves can actually ask for the certificates. Similar rules apply in Italy where pre-screening is not allowed except in the case of specific roles and duties, for instance in a financial institution. Credit and criminal record checks are forbidden.

With the globalisation of workforces, this is clearly a concern for some multinational companies. As Sarah Henchoz puts it: "If a company wants to hire someone in the UK who had previously worked in France, it simply won't be able to get access to the same kind of information. Not being able to check an employment history to the same extent, does make some companies quite nervous."

But Tobias Neufeld questions just how useful such checks are in protecting cybersecurity. "The situation in Germany is more restrictive than in the UK. But I don't see how vetting reduces the threat of a cyber attack or security breach significantly." German employers tend to rely, he says, on a much more exhaustive job applications process often supported by many reference letters from past employers and backed by laws that can make falsifying such letters a criminal offence.

Monitoring in the workplace – strict guidelines apply

65%

of large firms detected a cybersecurity breach or attack in the last year

Cyber Security Breaches Survey, 2016

Monitoring employees' emails, instant messages and internet use is another way to reduce data security risks. But in nearly all jurisdictions there are very strict data protection regulations on how this can be deployed – and, once again, there are important differences, from country to country.

These guidelines are usually very carefully laid out and backed by statute – in the UK, for instance, by the Regulation and Investigatory Powers Act 2000 as well as the interception of communications regulation. Under these rules monitoring is allowed for a range of specific business reasons including compliance with regulation or company policy, preventing a crime and to investigate unauthorised use of company IT systems.

Across the rest of Europe the rules tend to be a good deal stricter. Random monitoring is often forbidden and targeting an individual is often only allowed if there is a significant suspicion of serious misconduct. Companies overseen by a Works Council face an additional hurdle, on top of stricter regulation. Any monitoring policy will not only have to be clear, transparent and compliant, but may also often need to be sanctioned by the Works Council before being implemented.

In one further twist, German employers allowing their staff to use the internet for personal as well as work reasons are classified under national regulation as telecoms providers. As such, any attempt to monitor private communications becomes a criminal offence.

Recent high profile cases have shown, however, that the courts are prepared to take a pragmatic view of the balance between individual privacy and a company's need to safeguard security.

This was clear in the recent Bărbulescu v Romania case, tested in both national courts and ultimately at the European Court of Human Rights.

The case revolved around an employee who set up a Yahoo account at the company's request to deal with client enquiries.

Although company policies made it clear that such accounts were for commercial use only and that activity would be monitored, the company subsequently discovered the employee had been sending explicit messages to his fiancé via the account. When confronted, he denied the claim. So the company accessed the account to check his messages, subsequently dismissing him for breach of company rules.

The employee pursued the case through the courts claiming his rights under Article 8 of the Human Rights Convention (respect for private and family life) had been violated. But the ECHR concluded that the employee did not have a reasonable expectation of privacy when using the account and the company had the right to check employees were doing the work they were paid to do.

The judgment was justified on several grounds including the fact that the company had clear rules about personal use and had notified staff in advance that monitoring would be carried out.

"The case clearly shows that it is down to the employer to set the privacy expectations and to lay them out very clearly," says Sheila Fahy.

Inge Vanderreken agrees: "Companies' reasonable use policies need to be very clear. You need transparency, and monitoring needs to be proportionate and balanced. There's no unconditional right to do monitoring, but if you do it with transparency, and in line with local regulations, it is possible," she says.

"Many of our clients are now checking very carefully that monitoring for cybersecurity risks is sufficiently covered by their policies or if they need amending."

When crisis strikes

Given the growing incidence of security breaches in both large and small businesses, companies must ensure that they have contingency plans in place to deal with the inevitable and often devastating consequences in terms of trying to recover compromised employee or customer data, the threat of fines for breaching data protection rules, and the very real threat to a company's reputation.

"Organisations need to put in place a response plan in advance and that involves a team from across the organisation including IT, legal, HR, communications, security and compliance," says Ahmed Baladi. "It's a holistic approach and companies need to ensure they have built the right in-house resources and expertise."

Successful contingency planning and the ability to react quickly are essential. Sarah Henchoz recalls a significant security breach suffered by a client where an employee, possibly an industrial spy, stole huge amounts of data and attempted to flee the country.

The breach was quickly discovered and A&O lawyers worked closely with the company and the police to stem the leak within the first 24 hours. International arrest warrants were issued and private investigators were posted at airports around the world. Having missed him at one stopover, they caught him at another as he attempted to fly to a jurisdiction where it would have been very hard to extradite him.

"It was incredible how quickly we were able to work with the client and the police to limit the damage. With good contingency plans in place we were able to protect the company much better and also ensure appropriate action could be taken against the individual involved," she says.

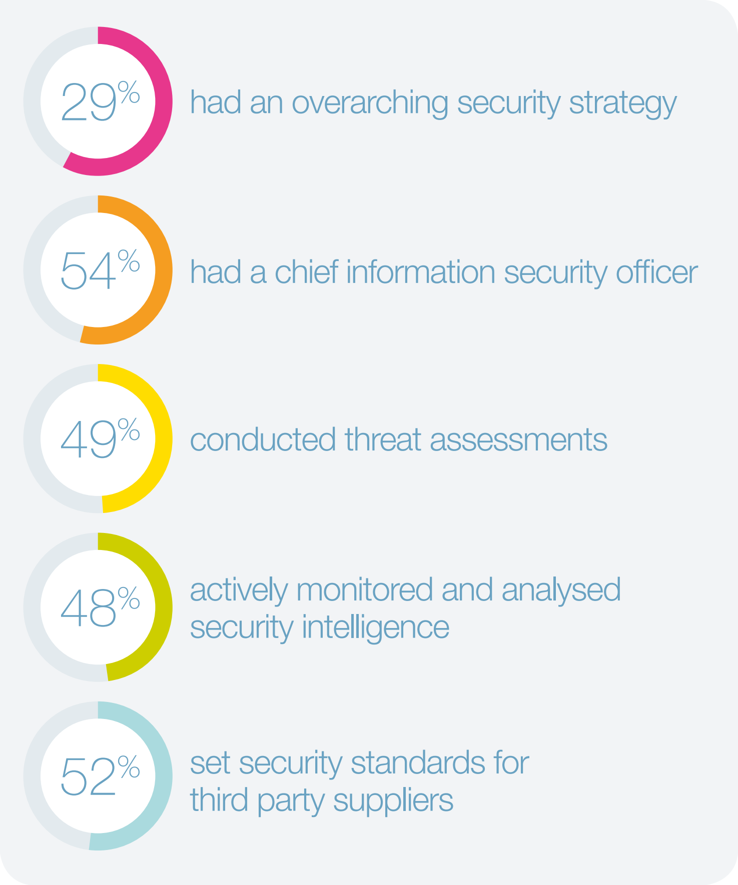
Increasingly clients call us in to help them stress test their cyber defences from every angle – and often in the aftermath of a breach. In one recent case, the dismissal of an employee found to be expressing extremist views and researching terrorist activities online at work led one client to begin, with our help, an end-to-end review of its approach to cybersecurity.

As Inge Vanderreken puts it: "What clients are looking for is a complete compliance test to check all their procedures from start to finish – IT systems, recruitment policies, workplace monitoring, education and training and contingency planning for a crisis – to make sure they are both as secure as possible and also compliant."

> *"It's a holistic approach and companies need to ensure they have built the right in-house resources and expertise."*
>
> Ahmed Baladi, Partner (France)

Reasons to be hopeful

There are, perhaps, grounds for hope that companies are beginning to respond to the threat – or at least treat it with the seriousness it deserves. But there's a long way to go. The PwC Global State of Information Security Survey 2016 found, for instance, that of the companies surveyed:



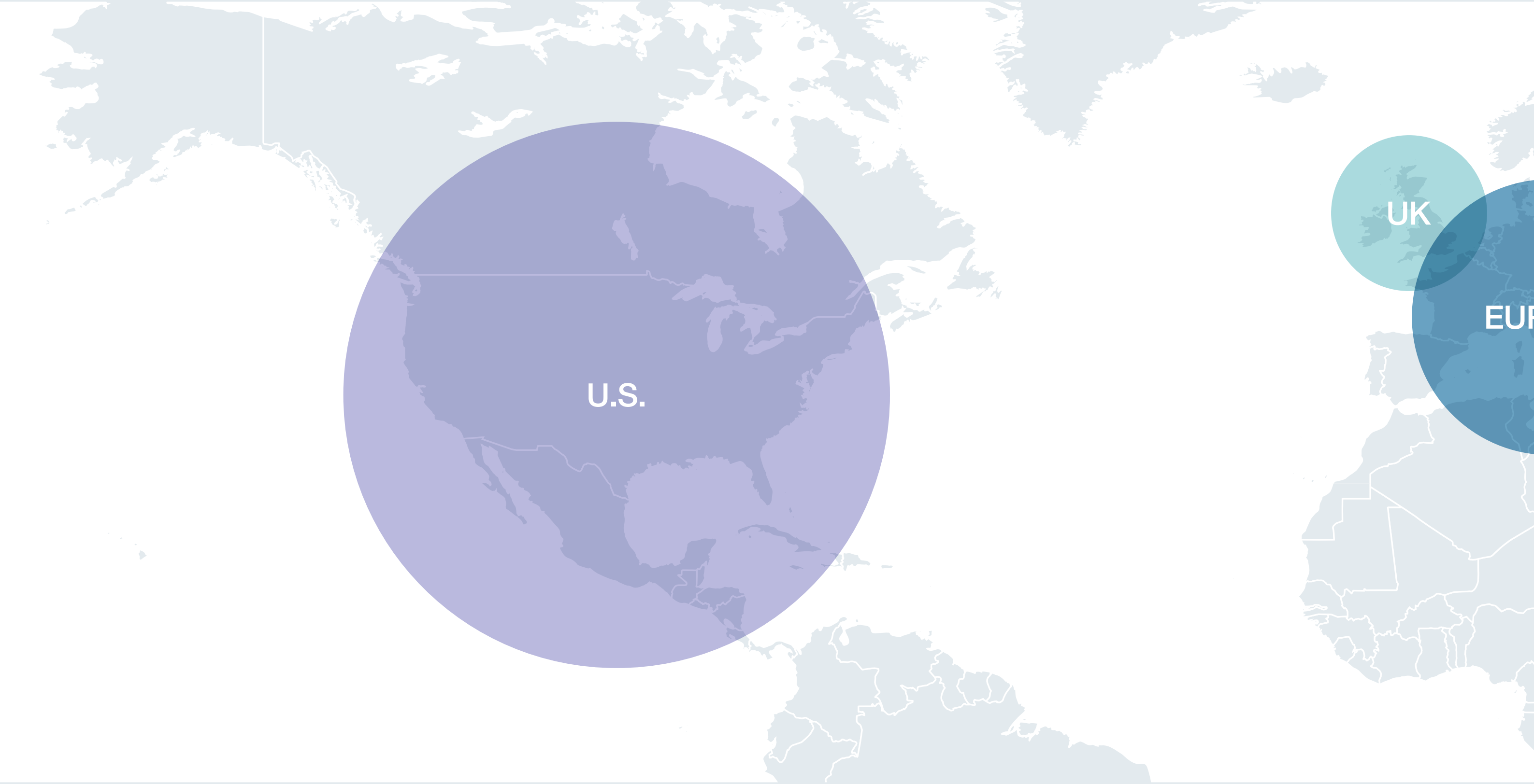
It also found that 53% of companies were conducting employee training and awareness programmes – clearly recognising how pivotal this work can be alongside other forms of defence.

As the cyber threat develops, that kind of work will be increasingly essential for all companies.

And as the war rages, many will find their own employees are their most important allies.

> *"One significant issue for multinational companies operating here concern the guidelines already in place restricting the transfer of information out of China, but no data protection regime, and no one agency, enforcing it. For companies used to much clearer rules and structures in Europe or even the U.S., this is creating uncertainty in an important marketplace."*
>
> Susana Ng, Counsel (Hong Kong)

Cybersecurity legislation



U.S.

Electronic Communications Privacy Act

Places restrictions on employee monitoring but provides exemptions including employee consent.

Health Insurance Portability and Accountability Act

Employee private health data is protected under this Act.

UK

Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

Authorises businesses to monitor or record communications on their own telecommunications systems without consent for specified purposes.

Regulation of Investigatory Powers Act 2000

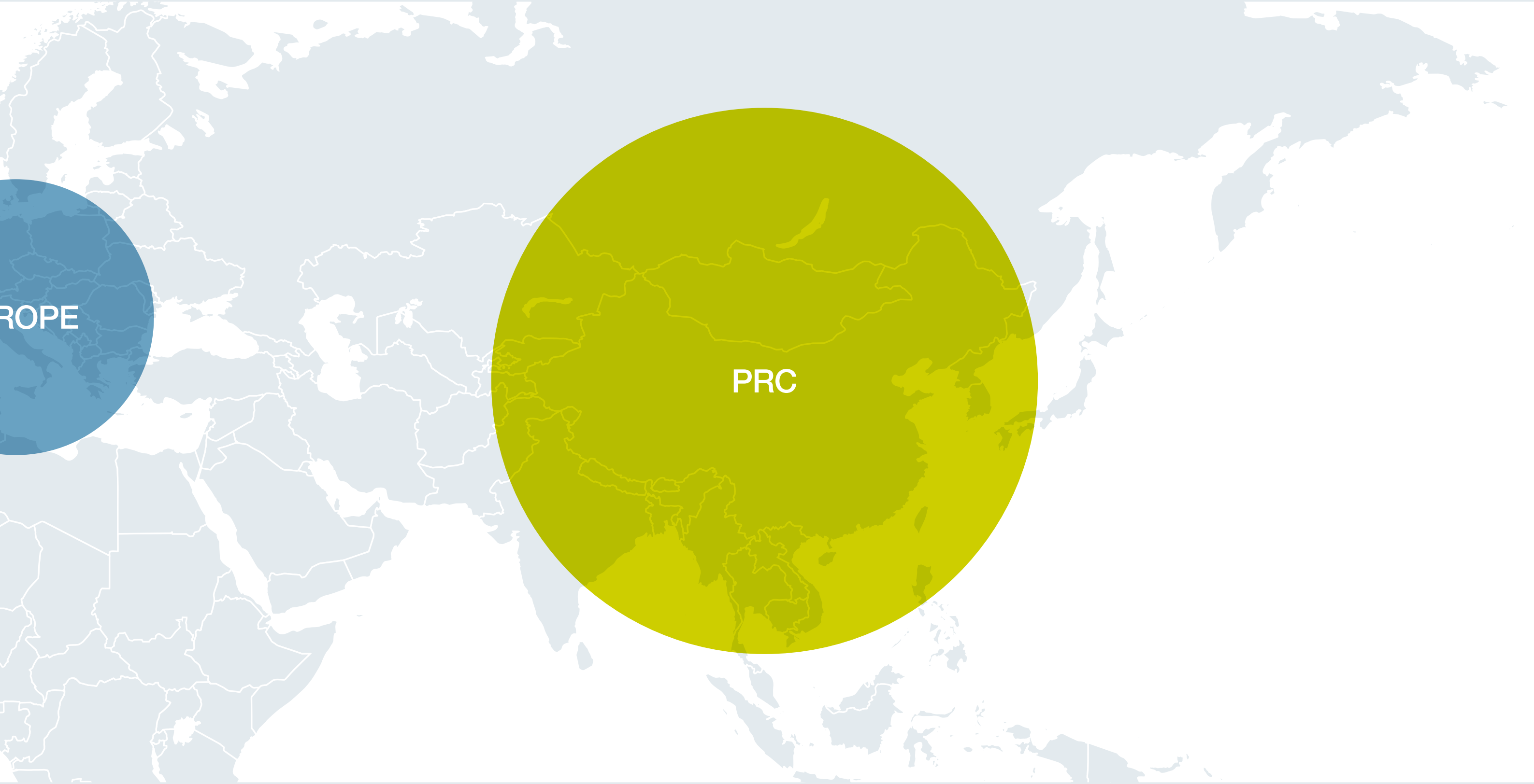
Legislation covering the interception (monitoring) of communications in the UK.

Data Protection Act 1998

Data Protection Act 1998 implements the EU Data Protection Directive and sets out rules governing the lawful processing of personal data.

Part 3 of the Employment Practices Code

Issued by the Data Protection Regulator to assist employers with monitoring employees.



EUROPE

Data Protection Directive

Data Protection Directive provides a regulatory framework, at a European level, for the protection of personal data.

General Data Protection Regulation (GDPR)

Onerous accountability obligations to demonstrate compliance; data controllers need to notify most data breaches to their local data protection authority; and penalties for breach of up to 4% of annual worldwide turnover – GDPR will be effective in May 2018 and will replace the existing Data Protection Directive.

Network and Information Security Directive

Aimed at companies in strategically important sectors (eg utilities), obliging them to report breaches to relevant national bodies and regulators – It is anticipated that the Directive will be in force in August 2016 and thereafter Member States have 21 months to implement the Directive.

PRC

(Draft) Cybersecurity Law

Aimed at conferring control over the internet and data on the government. Key industries, including energy, transportation and finance, are subject to specific regulatory requirements. Further, internet operators, including websites and social media platforms, are under a duty to report breaches to the authorities.

Contributors

Sarah Henchoz
Partner – UK
Tel +44 20 3088 4810
sarah.henchoz@allenovery.com

Tobias Neufeld
Partner – Germany
Tel +49 211 2806 7120
tobias.neufeld@allenovery.com

Ahmed Baladi
Partner – France
Tel +33 1 40 06 53 42
ahmed.baladi@allenovery.com

Livio Bossotto
Counsel – Italy
Tel +39 02 2904 9678
livio.bossotto@allenovery.com

Brian Jebb
Senior Counsel – U.S.
Tel +1 212 610 6354
brian.jebb@allenovery.com

Susana Ng
Counsel – Hong Kong
Tel +852 2974 7015
susana.ng@allenovery.com

Sander Schouten
Senior Associate – Netherlands
Tel +31 20 674 1641
sander.schouten@allenovery.com

Inge Vanderreken
Partner – Belgium
Tel +32 2 780 22 30
inge.vanderreken@allenovery.com

Sheila Fahy
PSL Counsel – UK
Tel +44 20 3088 3681
sheila.fahy@allenovery.com

If you wish to discuss this topic further, please feel free to approach your usual Allen & Overy contact at any time.

Previous publications

ALLEN & OVERY

The Big Think

How businesses cope with the rise of social media in the workplace.

ALLEN & OVERY

The Big Think

We look at the huge potential that employee and consumer data can bring to companies and their HR teams.

ALLEN & OVERY

The Big Think

International contributors look at the way a carefully planned and executed people management strategy can be critical to the success of a merger.

ALLEN & OVERY

The Big Think

Exploring the most prevalent new forms of employment, the legal constraints imposed by existing labour regulations and the legal challenges they present.

GLOBAL PRESENCE

Allen & Overy is an international legal practice with approximately 5,200 people, including some 530 partners, working in 44 offices worldwide. Allen & Overy LLP or an affiliated undertaking has an office in each of:

Abu Dhabi
Amsterdam
Antwerp
Bangkok
Barcelona
Beijing
Belfast
Bratislava
Brussels
Bucharest (associated office)
Budapest
Casablanca
Doha
Dubai
Düsseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Istanbul
Jakarta (associated office)
Johannesburg
London
Luxembourg
Madrid
Milan
Moscow
Munich
New York
Paris
Perth
Prague
Riyadh (cooperation office)
Rome
São Paulo
Seoul
Shanghai
Singapore
Sydney
Tokyo
Warsaw
Washington, D.C.
Yangon

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. The term **partner** is used to refer to a member of Allen & Overy LLP or an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP's affiliated undertakings.

All statistics taken from PwC Global State of Information Security Survey 2016