Anatomy of a breach

An Insight report on client attitudes to cyber security and how to respond when your defences fail
Anatomy of a breach

With breaches impossible to stop, companies are focusing on managing the huge risks of a major cyber incident. Legal Business teamed up with PwC to gauge the client response.

CHRIS CROWE

In cyber security circles, it has already become a hoary cliché to claim that there are two types of companies: those that have been breached and those that have yet to discover they have been breached. This rang particularly true this year when JPMorgan revealed that 76 million households and eight million small businesses were exposed to its data breach over the summer.

Banks are known to be among the most cyber and data secure institutions in the world, but even JPMorgan’s high-level defences couldn’t protect it from the increasing guile of cyber criminals. The frequency of breaches has led industry specialists to admit that such events often cannot be stopped, only managed.

Brian Dye, Symantec’s senior vice president for information security, declared earlier this year that antivirus ‘is dead’. For a company that was at the forefront of developing commercial software in this area, his comments illustrate the extent to which the cyber threat has moved on. Cyber defence technologies now largely focus on identifying a breach and then minimising the damage. If a banking titan such as JPMorgan can become a cyber crime victim, then what hope does the rest of the global economy have?

Philip Bramwell, group general counsel (GC) at BAE Systems, concedes that these are testing times: ‘We are acutely aware that increasing use of the internet, mobile working and the use of social media means that every organisation is at risk from a rapidly-growing range of cyber attacks.’

Bramwell says that maintaining information integrity and security is more challenging than ever. He favours a risk-based approach to cyber threats because ‘full security is not possible for most commercial organisations’.

Alastair Paterson, the chief executive and founder of Digital Shadows, the cyber threat intelligence company, says that businesses can no longer rely on firewalls and antivirus to protect their networks and data: ‘The first thing is to avoid a breach as best you can. You need to assess your own online profile, the risks you face and the techniques the attackers are going to use against you. It shouldn’t be a one-off exercise, but an ongoing process. You need to have plans in place so everyone knows what to do when a breach does occur. You need to quickly understand the nature and severity of the breach and be as open and honest as possible.’

To assess the extent to which cyber security has evolved within global corporates...
Aside from general counsel (GCs) and in-house lawyers having to take a greater interest in the cyber security environment, a new breed of specialist, the chief information security officer (CISO), is emerging in many big corporates. ‘The skills gap is huge,’ Stewart Room, head of cyber security and data protection at PwC Legal, remarks. ‘For the best quality CISOs, there is a real struggle to get the talent.’

Cyber security may have once been the remit of the chief information officer (CIO) or IT director, but it is clear that a basic technology response to the threats is no longer sufficient.

From a corporate strategy perspective, the approach has transferred from largely technological to one with a substantial human component. Top banks now have threat intelligence departments of up to 20 analysts, according to Alastair Paterson, chief executive and founder of cyber threat intelligence company Digital Shadows. ‘It’s very tough for most organisations to know what their risk profile is,’ he says. He adds that many FTSE 100 companies and financial institutions now employ former military intelligence and government agency workers as their CISOs or as other security staff.

The advent of the CISO role comes from the need to bridge the gap between the technology-facing part of the business and the strategic and operational element. The role is changing from a predominantly IT risk-focused position to one that is principally enterprise risk-oriented.

‘Organisations are now wholly dependent on their IT systems, making the CISO a critical connection between IT and the business,’ says Barry Coatesworth, CISO and industry adviser to the Department of Business, suggesting that CISOs are essential in protecting an organisation’s reputation and in enhancing client trust.

‘Due to an ever-increasing number of risks and responsibilities to deal with, as well as an increase in regulatory compliance requirements, the business case for skilled CISOs has risen dramatically,’ he says. ‘Organisations now understand that in order to deal with complex cyber security and risk issues they need someone at the forefront.’

While many CISOs have come from a technical background in the past, a new strain of professional is surfacing from the business side or from executive positions. They are required to balance security, business acumen and innovation, as well as build relationships and influence at executive level. William Brandon, the former deputy director of financial services strategy at HM Treasury, is poised to become the new CISO at the Bank of England in January 2015.

Steve Wright, chief privacy officer at Unilever, says that the modern day CISO must be capable of ‘managing up as well as down’ and talking to the business in business terms. Siân John, chief strategist EMEA at Symantec, agrees and says CISOs must try to be detached from the IT team: ‘It’s becoming a more senior role and with increasing salaries. It’s not about buying bits of technology and sticking them on the network.’

However, industry experts believe that businesses should do more to coalesce skills and expertise from within the organisation. CISOs and GCs could be more collaborative, especially as cyber crime is essentially an alien subject to most legal heads. And unlike the CIO, CISO and in-house counsel have common ground in being primarily charged with managing risk.

However, so far there has been a problem of silos and a lack of trust and communication between in-house legal teams and CISOs. PwC’s Room argues that GCs need to bridge that gap and the best course for heads of legal at large bluechips is to cultivate their CISO or closest equivalent well before a major breach, when the involvement of legal teams can make colleagues defensive.

David Pinkney, GC at NTT Europe, believes there is increasing collaboration between information security specialists and legal departments. He and the information security officer (ISO) at NTT sit on many of the same internal committees. ‘We see each other all the time and work very closely together.’
and discover the extent to which GCs are involved in the process, Legal Business teamed up with PwC to garner responses from over 800 clients and spoke to a number of senior in-house lawyers to get their perspective on managing the growing legal risk of a cyber security breach.

**THE POINT OF ATTACK**

Cyber criminals have clearly got the upper hand over traditional business defence methods, evidenced by the regularity of headline breach stories. The Ponemon Institute, an independent research organisation on privacy, data protection and information security policy, published its annual survey in October 2014 arguing that cyber crime cost the average UK business £3.56m, an increase of 17% on the 2013 survey.

Two standout incidents in the last 18 months were those suffered by Target and The Home Depot in the US. In December 2013, Target, the US retailer, suffered a huge data breach in which millions of customers’ credit and debit card details were compromised. On 10 January 2014, the company admitted that it had lost the personal data – including names, phone numbers, and e-mail and mailing addresses – of some 70 million customers. The incident led to the resignation of chief executive Gregg Steinhafel in May, following the departure of chief information officer (CIO) Beth Jacob in March.

Meanwhile, The Home Depot, the DIY chain, suffered a gigantic breach in the spring of 2014 when cyber criminals hacked into its payment terminals, leading to millions of credit card accounts becoming compromised.

In Europe, the story is equally worrying. Examples of organised criminals employing hackers are rife, as exemplified by the Port of Antwerp breach that came to light in 2013. Drug traffickers hired hackers to breach the IT systems of companies operating within the port and then were able to identify and move containers that were holding drugs in among legitimate cargo. The attack is thought to have been carried out over a two-year period, in which the traffickers were able to send in lorry drivers to steal containers that were holding the drugs, before being detected.

Such events are contributing to a fast-moving and alarming narrative, which is increasingly attracting the attention of the legal profession.

‘Cyber security has come from nowhere to the forefront of people’s attention,’ admits Derek Walsh, group GC at RSA.

Robin Saphra, Colt Group GC, says that cyber security has been more of an operational and technological concern traditionally, but it is becoming a source of anxiety for his department: ‘It is probably right up in the top quadrant of my legal risk matrix. It has absolutely got the attention of the board and management, as well as the attention of the Colt legal community.’

Kris McConkey, the head of the cyber threat detection and response team at PwC, highlights a particular instance when cyber attackers managed to access a business’s disaster recovery plan, and then contacted the telecoms provider to redirect the phone lines. Having done this, they were able to authorise illegitimate bank transfers.

This instance demonstrates the extent of the planning and execution process that the hackers go through to perform such a flamboyant crime, a felony worthy of a Hollywood feature film.

‘Every organisation is at risk from a growing range of cyber attacks. Full security is not possible for most firms.’

Philip Bramwell, BAE Systems

PwC Legal, an integral part of the PwC international network of firms, is a leading law firm with expertise in cyber security, data protection and privacy, intellectual property, human resource services, corporate finance, tax, and financial services regulation. We provide clients with a distinctive approach of integrated legal advice on complex commercial projects requiring a range of complementary specialists from other parts of the PwC network. We also offer clients a general counsel service and access to an extensive global network including locally qualified legal expertise in over 80 countries.
The difference today is that hackers take a ‘low and slow’ approach to their cyber attacks, according to Siân John, chief strategist EMEA at Symantec. Cyber criminals study their intended victim, gather as much information on them as possible, including their business partners, suppliers and anything that will enable them to identify a weakness in their defences. Hackers analyse and plan over a number of months, or years even, so that they can maximise the result of the attack.

It is no longer a smash and grab scenario, as Stewart Room, head of cyber security and data protection at PwC Legal, comments: ‘They’re surveying the network to try to find a chink. Once they find the chink it is like water in the rock. When the water is there it freezes and the rock starts to crack. They may spend many months watching the network and understanding how it works before planning the great big attack. They break in first and they start to plan. So they could be on the network and then do the grab overnight and then erase it behind the scenes.’

DEALING WITH THE INEVITABLE
Even with a substantial threat intelligence department, businesses may struggle to identify a breach and immediately deal with it. JPMorgan’s data loss is a case in point. Breach prevention is futile, according to many industry experts, who suggest that detailed breach response planning is a more effective approach.

Stephen Bolinger, chief privacy officer and vice president in the legal department at LA-based internet security company TeleSign, says that dealing with breaches requires substantial internal organisation: ‘If you are trying to come up with a process on the fly, you are just going to make far more mistakes.’

CPA Global’s GC Ruth Daniels says it is important to understand the impact of the breach and how it might affect business operations: ‘What are the legal consequences with regards to contracts and notifications? What regulatory requirements kick in? Finally, damage limitation through a proper communications plan is critically important.’

Many corporates still have hundreds of unencrypted laptops that could fall into the hands of criminals. An obvious way of minimising the effects of a breach is to compile an accurate and up-to-date asset list, so that if any devices go missing they can be quickly detached from the network.
Orion Hindawi, the co-founder and chief technology officer at security and systems management company Tanium, also says that businesses should stop worrying about the stigma of being associated with a breach and become known as the company that addressed the event in the appropriate fashion. He references JPMorgan’s reaction to its breach as one of the more effective responses. ‘Every company is being attacked and JPMorgan decided to disclose this attack out of good hygiene,’ he comments.

The investment bank’s chief executive Jamie Dimon has since talked openly about the event and how the industry can respond and work together and was widely quoted in October as saying the bank would spend $250m a year to increase security. ‘This is going to be a big deal and there will be a lot of battles,’ he said. ‘We need a lot of help.’

Beyond openness, industry specialists advocate a proportionate and multidisciplinary tactic to dealing with a breach. Symantec’s John says: ‘You don’t deal with risks by turning off all the computers and turning off the internet. You look at a lot of the breaches where it has gone wrong. It has gone wrong because the communication hasn’t gone well. You may have a technical response, but if you’re not communicating it well, it has an impact on your reputation.’

LEGALLY PRIVILEGED
When it comes to deciding whether to report a breach to regulators, to customers and to the press, understanding the nature of the event is imperative. GCs, in-house lawyers and external legal professionals may be well equipped to decide on what should and shouldn’t be reported, but their role and skill are also paramount in discovering the facts of any cyber breach.

The regulatory landscape is also moving towards mandatory breach disclosure and substantial fines for not meeting the directives (see ‘Cyber security – the regulatory landscape’, page 82), putting further demands on the legal department in a breach situation.
‘Cyber security has come from nowhere to the forefront of people’s attention.’

Derek Walsh, RSA

In addition, many breaches occur thanks to human error, according to Steve Wright, chief privacy officer at Unilever, meaning responses need to take account of issues like human resources, and forensic investigations that involve digging into the network and looking through e-mail boxes. Searching for a rogue insider or perhaps dealing with an employee that has fallen victim to a phishing attack are other situations that require legal judgement.

In these instances, the data and cyber security specialists, such as the chief information security officer (CISO) and CIO, do not usually possess the requisite skills.

Charlotte Heiss, RSA’s head of legal, says that approaches to cyber risk and financial crime need to be broken into three key categories: ‘What are the potential risks, which regulations govern what, and how do we establish a framework to mitigate against those risks and ensure we comply? How do we implement appropriate systems and processes to ensure that we are appropriately protected and compliant? And, lastly, how do we manage the fallout if something goes wrong?’

She believes that the first and third questions are where the legal team can

---

1. No; 2. Yes - with legal counsel and within the past 12 months; 3. Yes - with legal counsel but over 12 months ago; 4. Yes - within the past 12 months but without legal counsel; 5. Yes - over 12 months ago and without legal counsel; 6. Yes - other

1. No; 2. Yes - other
provide genuine added value, but that the second question requires the ‘lion’s share of the work’.

With the prospect of a new European regulatory environment attaching fines of 2% of a business’s global turnover for failing to meet EU rules, then these legal judgements do have considerable value.

Room says that the tool of legal privilege is often pivotal to understanding the nature of the breach, and the damage to the business. ‘Often you need professional privilege to get to the truth. I’ve often noticed that there is a very clear blame game going on. And where we have a regulatory issue as well, when people are fined, it is all about blame and liability isn’t it? Blame and liability are really unhelpful when you are trying to get to the truth of things. It causes people to filter their evidence. If you are interviewing a witness and the witness believes that they are going to be blamed or sacked, you have to penetrate that filter. Privilege can give more comfort and encourage truth telling. As an external lawyer you also want to play devil’s advocate with your client. You want to test the client’s case as hard as you can and testing is something that needs to be done in a privileged environment.’

Evidently, these legal skills have an anchor role to play in these increasingly
Global regulation of data protection and cyber security is moving towards a mandatory disclosure environment. This includes significant fines for flouting the rules.

In January 2012, the EU published its Draft General Data Protection Regulation, which levies mandatory breach disclosure on any organisation that holds data in the EU. The proposals are expected to come into force within the next 12 to 18 months, though the mandatory disclosure rule has already been in existence for telecoms providers and internet service providers since 2009.

In addition, de facto mandatory breach disclosure rules for public sector entities have been in existence in the UK since 2007. This followed an infamous HMRC data breach, when two data discs holding the personal details of all families with children under the age of 16 went missing.

A worrying prospect for those that fail to comply with the new EU regulations is the maximum fine of 2% of global annual turnover. ‘It could get quite painful very quickly,’ comments Siân John, chief strategist EMEA at Symantec.

This form of regime is already in existence in the US, where all federal states have a mandatory breach disclosure policy. In October, TD Bank paid an $850,000 settlement following its reported loss of unencrypted backup tapes that held personal information on 260,000 customers.

However, the new European regulations are broadly welcomed because they will provide some legal consistency across the EU. Stephen Bolinger, chief privacy officer and vice president in the legal department at TeleSign, says that the regulatory environment in the US has become especially complex because the individual states have enacted their own breach notification requirements, leading to a patchwork of directives from state to state. He explains that the individual ‘quirks’ in each state’s legislature has led to a cottage industry of organisations that provide maps and charts of the complex regulatory landscape across the US. The US National Institute of Standards and Technology (NIST) is in the process of developing a broader and more harmonious framework for cyber security policies to be based on.

At present, multinational companies face troubled and uncertain surroundings. Operating across regions poses a significant challenge for businesses to meet regulatory and legal requirements of the jurisdiction where they are incorporated and the nations where they operate.

Barry Coatesworth, chief information security officer (CISO) and industry adviser to the UK’s Department of Business, observes: ‘This can be challenging when developing cyber security policies, as there can be conflicting requirements, which can add extra burdens, cost and complexity for compliance.’

Coatesworth also suggests that there is an obvious tension between the US regime and the EU’s proposals: ‘One of the more obvious conflicts is the US Foreign Account Tax Compliance Act (FATCA), which requires a level of transparency with transferring personal identifiable information to the US. This conflicts with the new European Data Protection Regulation, where the EU commission has issued an official statement stating that the US does not offer an adequate level of protection.’

‘Just being compliant in the security sense does not necessarily mean that you are secure.’

‘Often you need professional privilege to get to the truth. You want to test the client’s case as hard as you can and testing is something that needs to be done in a privileged environment.’

Stewart Room,
PwC Legal

ubiquitous cyber breaches. And GCs and in-house lawyers are recognising their own worth in such scenarios. Saphra comments: ‘I would say a big role is where there is an event or a risk of an event and there is a very clear line that needs to be navigated. For example, how do you communicate with your customers and regulators, and how do you work with the police? That has to be navigated by the legal counsel. Where there is a crisis, I am very much part of the core response team.’

Chris Fowler, UK commercial legal services GC at BT, agrees: ‘There will be an ongoing focus on contingency planning to identify all the potential internal and external implications of an actual or potential breach.’

Yet according to our survey, only a fraction (16%) of legal teams are heavily involved in the drafting and review of security and contractual framework policies. Furthermore, only 34% of respondents have considered the role of legal professional privilege during an incident response.

GCs and in-house legal departments outside of the US have been somewhat detached from the cyber crime phenomenon. Cyber security has a short history and it has yet to capture the attention of the broader legal community. RSA’s Walsh says that while cyber attacks will almost certainly
‘Cyber security is probably right up in the top quadrant of my legal risk matrix. It has absolutely got the attention of the board and management.’
Robin Saphra, Colt Group

become a grave concern for GCs, it has yet to be a prime topic of conversation: ‘When I meet with FTSE 100 GCs, they are really good at identifying issues affecting the industry. Cyber security is not at the centre of our discussions. It’s just not falling into the responsibility of the GC yet.’

McConkey says the scene is very different in the US: ‘The GC is front and centre, mainly because they have a role in protecting the company, especially if it goes down the route of involving the regulator. In the UK it is extremely rare that we get calls directly from GCs. They will sometimes be involved in incidents, but they are not typically leading an organisation’s response to an incident. It is much more likely that we will get a call from the CIO or CSO.’

Despite having few cyber security conversations with his GC peers, Walsh recognises that attitudes towards
The good news in the longer term is that there are signs of international trends emerging in legislation in the area that promise to ultimately see clearer standards emerging. The global development of regulation and law in cyber security has so far demonstrated several trends: aside from increasing expectations for companies to come clean in the event of a breach, specialists in the area expect more common ground on what is expected of companies and advisers in terms of legal duty of care.

Traditionally the US and the UK governments have been among the most progressively minded states in terms of building effective cyber legislation, regulation and encouraging companies to take the issue seriously. Cited in this context as a useful benchmark is the UK government’s ‘cyber challenge’ ‘10 Steps to Cyber Security’.

But if there is good news for GCs in that more commonly-used standards are emerging, a separate challenge is that the complexity and the body of knowledge being rapidly built up means that, in the words of PwC Legal’s Stewart Room, regulation is moving beyond the broader policy stage, where it was dealing with softer thematic issues, towards a harder phase, where it is dealing with granular technical and practical issues. GCs, even when they are focused on cyber security, tend to focus on policy rather than the technical issues that Room argues will be increasingly driving the process. While most sector specialists acknowledge the need for a clearer and more congruent regulatory landscape, they warn that businesses that simply meet the minimum requirements are still likely to be soft targets for cyber criminals.

Kris McConkey, the head of the cyber threat detection and response team at PwC, says that major breaches have occurred in companies that met the IT service management standard ISO 20001: ‘There are a lot of standards out there and what clients need to realise is just being compliant in the security sense does not necessarily mean that you are secure. They are useful as good practice guides, but in no way is this going to defend an organisation.’

He suggests that there should be greater collaboration between competitors in each industry sector, a sharing of knowledge and a move towards intelligence-driven security.

Another substantial challenge for those engaged in the cyber security environment is the speed in which it is evolving. While the authorities are trying to create a landscape in which businesses can clearly understand their obligations, the danger is that cyber criminals are constantly three steps ahead.

Robin Saphra, Colt Group GC, says that a company must do its own groundwork: ‘My concern with regulation is that it is sometimes behind the curve. Regulation is struggling to keep up with the dangers and there is a risk that it tends to address technology that is already obsolete. Regulators are doing a better job than they used to, but there is a very important place for self regulation.’

> the importance of legal expertise in responding to cyber threats will need to change. He suggests that the regularity of cyber attacks and the evolution of the tighter regulatory backdrop will lead businesses to seek out additional legal knowhow. But is the legal profession properly equipped? Only 21% of our respondents said that their external legal advisers are very capable of handling a serious cyber security incident.

Walsh concludes: ‘I think in 2015, we will be talking about cyber security frequently. What we care about is what will be the interpretation of the rules and law firms can be very slow at doing that. I would suggest that lawyers get on the front foot with offering practical advice rather than repeating what the rules state because we can read those ourselves.’

Bramwell goes one step further. He says that GCs will remain ‘front and centre stage in the board-level management of cyber risk issues’, but he believes that they will have to look more closely at what controls their external legal advisers have around client data. Those at the top of the supply chain will be setting the cyber security benchmark and suppliers and professional services providers will be expected to meet the necessary standard. Any that fail to address cyber threats or respond to them appropriately will suffer the consequences. LB

### INSIGHT: CYBER SECURITY

**The Regulatory Landscape**

Despite increasingly stringent legal requirements, business operations continue to cause threat, according to a survey of 830 respondents.

1. No - we do not have a cyber security policy;
2. Yes - we have a cyber security policy and it is updated and in line with regulatory changes;
3. Yes - we have a cyber security policy and it is updated and in line with regulatory changes and enforcement.
4. Don’t know

Room argues will be increasingly driving businesses to look more closely at what controls their suppliers and professional services providers have around client data. Those at the top of the supply chain will be setting the cyber security benchmark and will be expected to meet the necessary standard. Any that fail to address cyber threats or respond to them appropriately will suffer the consequences.

### METHODOLOGY

Legal Business polled major companies on cyber security in late October, receiving 830 responses. The breakdown of respondents came from a diverse range of roles within companies, with around a third occupying in-house legal roles such as GC, another third were individuals in senior board level positions, such as chief executives, managing directors or owners; while 26% chose other, including roles such as heads of IT, risk and compliance.
Building confidence in your digital future

Our multidisciplinary cyber security team, which unites PwC and PwC Legal capabilities, advises organisations large and small in every sector of the economy. We provide a broad range of integrated, end-to-end cyber security services with specialists offering risk assurance, forensic, legal, technology, and people and change consulting services designed to provide our clients with the confidence they seek. We are equipped to help organisations with detailed data and technical analysis, and equally, we can advise senior management and boards in shaping a broader strategic response to cyber security risks.

Our specialists help organisations reduce their exposure to cyber threats and to improve their defences. Through our Breach Aid service we provide multi-disciplinary support to clients to help them respond to cyber incidents quickly and efficiently. We also address the legal issues around breaches, data privacy and protection, as well as help with implementing the requisite culture and environment where your people understand how to behave and do the right thing.

Our Cyber Threat Operations team – which includes incident response and threat intelligence – guides and supports organisations dealing with sophisticated cyber attacks, including advanced persistent threats. Combining PwC’s technical know-how with PwC Legal, we offer our clients an unparalleled cyber security service. Our legal experts are market leaders in the practice of cyber and data security and privacy law, with practical industry and regulatory knowledge. Our legal capability also enables us to offer our services under legal professional privilege.

We understand that cyber security is a multi-faceted issue that requires deep understanding, agility, timely execution and empathy. Our service offering brings together the breadth of capability that clients need to operate as an integrated team, and manage cyber security matters with confidence. We are the catalyst advising chief information security officers (CISOs), chief information officers (CIOs) and boards in the effective discharge of their responsibilities to deal with disruptive business impacts such as cyber security. Our focus is to help our clients find the right solution and to add value to their business.

We are the safe pair of hands trusted by government and industry to handle some of their most sensitive issues. With PwC offices in 157 countries, we are confident that our international network can provide our clients with local and global expertise and support they require.