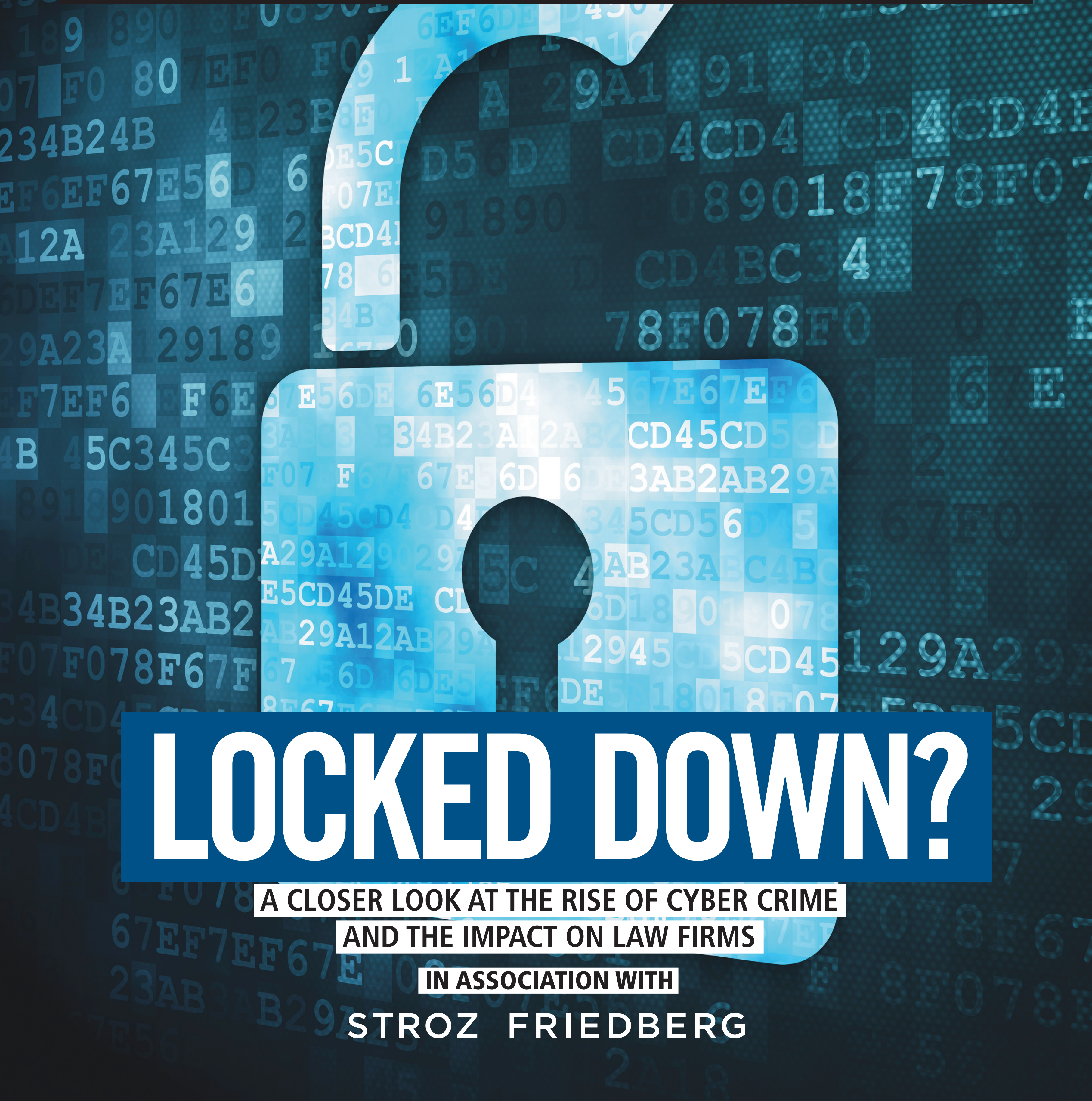
BENCHMARKER
Legal Week

Legal Week Intelligence

CYBER CRIME

3 May 2013

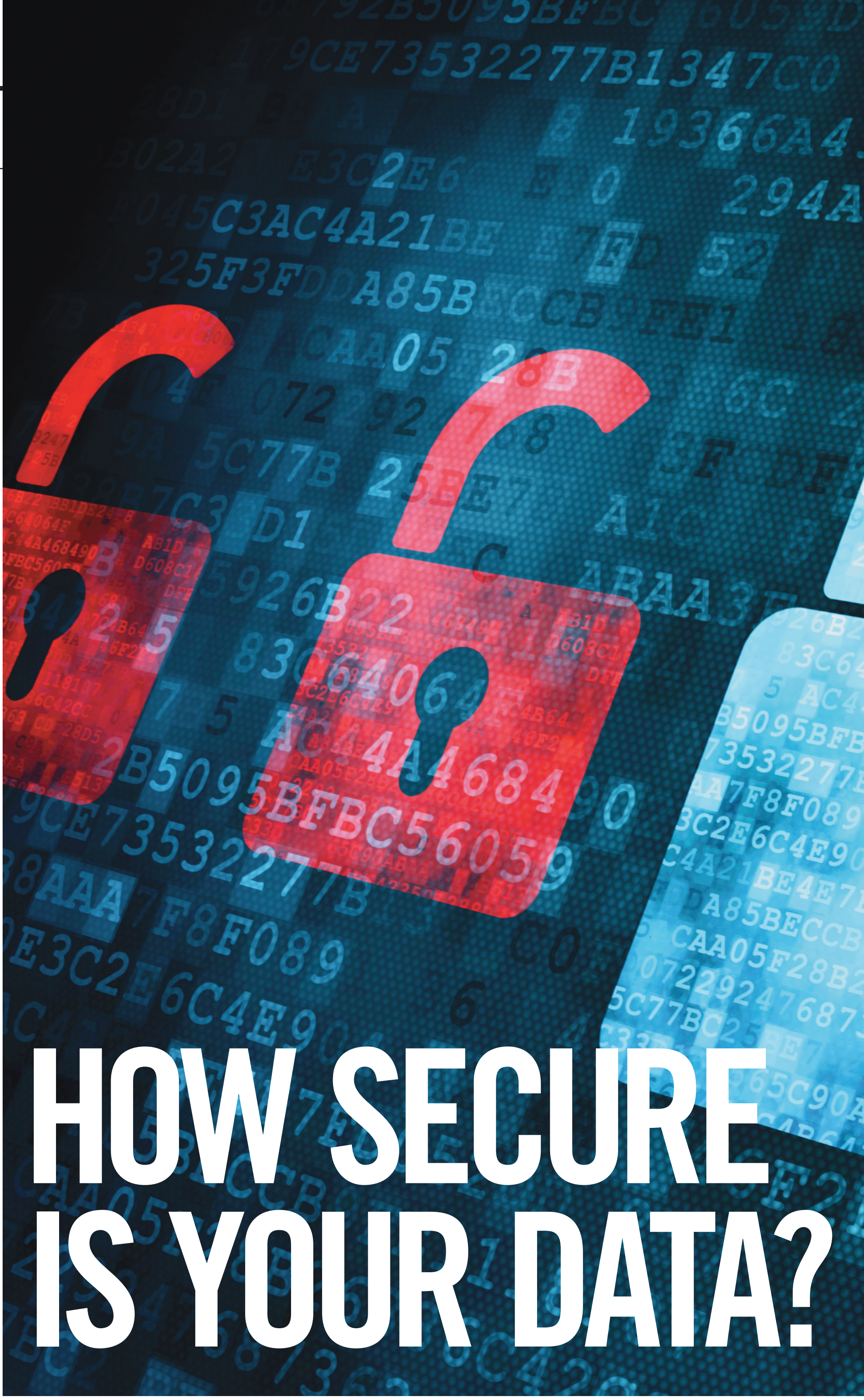


LOCKED DOWN?

A CLOSER LOOK AT THE RISE OF CYBER CRIME AND THE IMPACT ON LAW FIRMS

IN ASSOCIATION WITH

STROZ FRIEDBERG



HOW SECURE IS YOUR DATA?

The latest Legal Week Benchmarker study, in association with Stroz Friedberg, takes a look at the ways firms are tackling the growing problem of cyber crime. **Neasa MacErlean** picks out the key results

Two-thirds of senior executives believe their sector is attractive to cyber hackers, according to recent research.

Legal Week's latest Benchmarker survey, which canvassed the views of more than 370 senior business people, of which almost half worked in the legal profession, also found the majority of chief information officers (CIOs) felt the number of these attacks is growing.

Seth Berman, executive managing director of Stroz Friedberg in London, has a warning for everyone: "Even the best computer security can be breached. It is not a matter of if; it is a question of when."

This shocking conclusion fits in with other research that Legal Week Intelligence has carried out. Our IT Report 2012 showed that 20% of the 51 firms that took part in that survey, including three magic circle practices, had been attacked in the previous 12 months.

As we said in that report: "There is no correlation between poor systems and being attacked. In fact, the correlation may work the other way at the moment: the firms which are most at risk (because they have the clients which are most at risk) probably tend to be those with the best defences. These firms are likely to have built up their systems in order to ensure that they attract those clients."

Cyber security is such a sensitive subject that many CIOs in law firms do not want to address it on the record. Several have been briefed in the past year by the UK security services and they know that the stakes are high. But one law firm CIO, who wants to remain anonymous, told us: "There are a lot of sensible people telling us all sorts of scare stories. If a foreign government were looking at our systems, I don't think we'd ever know. If you have got 30,000 people in China involved in espionage and they want to know what our position is, because we are acting for the other party, I don't think that my much smaller team could fend them off."

It is a clear that the incidence and severity of cyber attacks is increasing. Recent victims include JP Morgan Chase, American Express, Australia's central bank and HSBC. Berman believes that law firms will have to pay more attention to cyber security.

"The failure of UK law firms to tackle online security is leaving clients increasingly vulnerable to attacks. As custodians of clients' intellectual property and commercially sensitive information, law firms are particularly attractive to hackers. We know law firms are being targeted," he says.

Law firms may feel that they are unlikely to get caught in the cross-fire between hostile states and the media outlets of the west – but financial institutions have been taken by surprise on this one too. On top of that, hackers seeking commercial secrets are known to regard law firms as a weak link in the information chain. "The very nature of law firms makes them an active target," says Berman.

At the very least, professional practices want to avoid tarnishing their reputations by clashing with regulators over data management. In order to help solicitors avoid compromising themselves and their clients, the Law Society announced in April that it is opening a consultancy to advise firms as well as setting up "a cyber security community of interest, which will allow firms to come together to confront the threat". Sharing information is being encouraged by UK and US authorities and is seen as one of the best means of defence.

In our IT Report 2012, the top mark that the IT teams of law firms received across the whole range of their services to fee-earners came on security. Law firms have worked hard on this issue but the real concern is that many hackers are working even harder. Realising

that the business community was unaware of the real nature of the cyber threat, the security services are determined to improve understanding. We are now seeing a flurry of initiatives, including the Information Commissioner's new guidance on the BYOD (bring your own device) issue.

Across the pond, the Americans are very active. For instance, the American Bar Association introduced a new rule last August which aims to protect against inadvertent disclosure of client information.UK law firms will also find themselves under pressure from their own clients. James Watson, director of legal at media

Continued on page 16

KEY FINDINGS

- Non-lawyers are far more likely (52%) than law firms (35%) to have a response plan in place for cyber attacks.
- Over two-thirds of law firm personnel (68%) think that the law is an attractive target sector for cyber criminals.
- Three quarters of employees in law firms with annual turnover above £500m think they are likely to be the subject of cyber attacks.
- Nearly four in ten people working in the legal sector (38%) believe that the number of cyber attacks is increasing.
- Only 10% of law firm personnel think that UK businesses are ready to deal with cyber risks.
- The biggest concern about a cyber attack for law firms is potential loss of client data (32%).
- Law firms lag behind the rest of the commercial world in terms of estimating costs of a cyber attack. Only 9% have worked out potential costs – compared to 26% in businesses outside the legal sector.
- Legal practices with between 5,000 and 9,999 employees are particularly concerned about hacking by state entities (42%).
- Lawyers are nearly twice as likely (13%) to suspect their own employees than those outside the legal profession (7%).
- Less than a third (31%) of people working in law firms believe that their top management fully understand the issues around cyber security, compared to 36% outside the law.
- Just over a third (36%) of law firm personnel think their systems can withstand attacks – lower than the 43% registered for other types of organisation. Confidence sinks to 24% in legal practices with between 500 and 999 employees.
- Two in three respondents from law firms (62%) think that their business partners take the cyber threat seriously.
- Nearly two-thirds of law sector respondents (58%) would information-share with other organisations.
- The vast majority of lawyers (86%) see cyber security as an issue for the senior executives.
- Law firms (60%) are more likely to have addressed the risks of iPads and other portable devices owned by their personnel than those outside the law (53%).
- Legal practices (51%) are slightly less likely than the average (53%) to have addressed cloud security issues.
- Partners and staff in law firms are markedly less supportive (53%) of compulsory reporting than those outside the legal profession (65%).
- Respondents from the legal sector are less likely (35%) to include external cyber security experts than non-lawyers (53%) in their attack contingency planning.

CASE STUDY

A UK law firm was recently the target of a spear phishing attack, which is a highly targeted form of phishing. The hackers created an email address in a name that looked very similar to the name of the firm's managing partner, which was followed by an email to every associate in the firm.

The email, purportedly from the managing partner and sent after hours, asked the associates to review a document so that they could discuss it in the morning, and explained that he had to use his home address because he could not access the firm's network at that time. The document contained a virus. All associates who opened the attachment unwittingly downloaded the virus onto their computer and from there into the firm's network.

Continued from page 15

and entertainment company Deluxe, says that the possibility of their external lawyers being hacked "is a concern" for in-house counsel. He adds: "I expect more clients to take an interest in their external advisers' security procedures."

The CIO of a large law firm echoes Watson's comments: "The issue of cyber terrorism and espionage has really gone up the agenda of law firms. Large corporates now have a huge focus on this area and we need to ensure their interests are protected."

Berman adds: "The failure to address such threats, as part of an ongoing process of review, testing and training, could have significant business continuity, cost and reputational implications."

Does the board understand the risks of cyber attacks?

Law firms are less convinced than other respondents that their senior executives understand cyber risk. Only 31% believe that their leaders fully understand the issues, compared to 36% outside the law.

Respondents working in the law have more faith in their top management than accountants (20%), but significantly less than those in financial services (45%) and business services (56%).

Measured by length of payroll, law firms with between 500 and 2,499 personnel have the lowest level of confidence in their senior managers (24%) while larger practices are more trusting.

The head of a small City organisation is clear that cyber threats need to be discussed at top level: "There was a piece of litigation we were involved in recently where our lawyer gave us a 50-50 chance in an email. That would have encouraged the other side a lot if they had access to that."

Some of these attacks have been claimed by terrorists as their work. The Al-Qassam Cyber Fighters group said that the 'denial of service' attack on Amex – which took the Amex site offline for two hours – was its work, a way of putting pressure on YouTube to take down an anti-Muslim video. But some experts believe this attack was so sophisticated in nature that it may have been state-sponsored from Iran.

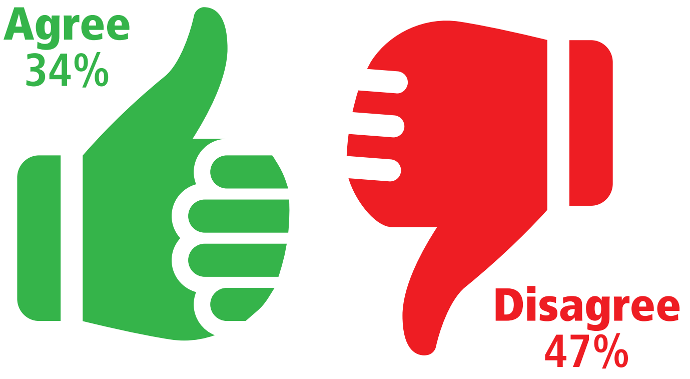
Does your industry sector feel safe?

Legal practices think they are slightly more prone to attack than other respondents. Only 22% think the law is "unlikely" to be an attractive target – slightly lower than the 24% of other organisations which rate their sectors as unlikely to be targeted.

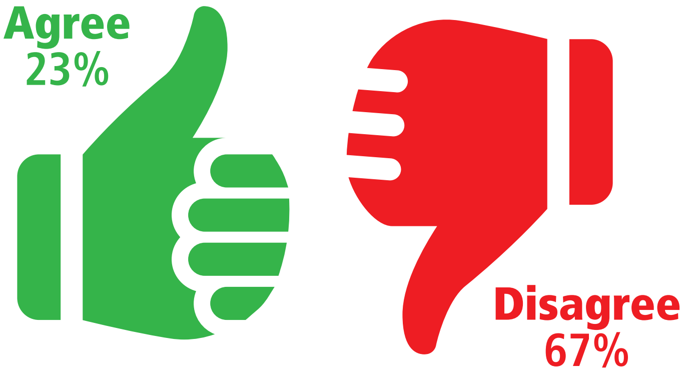
Those working in financial services are more concerned than lawyers about being attacked – with only 19% thinking it unlikely they will be targeted. People

> **"The failure of UK law firms to tackle online security is leaving clients increasingly vulnerable to attacks. We know law firms are being targeted"**

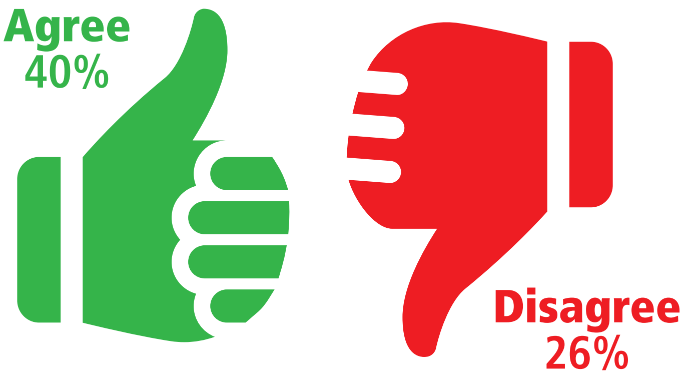
Board-level managers fully understand the risks posed by cyber attacks



Our industry sector is unlikely to be an attractive target to cyber criminals



Our IT systems can withstand an external cyber attack



from business services (39%) are relatively unfearful. By turnover, the law firms which are most concerned are those with turnovers above £500m, where at least 75% think attacks are likely.

Least worried are those with revenues below £10m, where the fearful contingent represents 64% of respondents.

Stroz Friedberg's Berman says: "The decision by the FBI to bring together 200 New York law firms for a threat briefing underscores the heightened risk of cyber attacks and hacking. In my experience, there is also some way to go before the cyber security challenges facing UK law firms are fully understood."

Clients will put more pressure on law firms to improve their defences, in Berman's view: "Clients will increasingly be looking to their legal advisers for leadership and reassurance that steps are being taken to reduce such risks."

Deluxe's Watson wants law firms to stay extremely vigilant. "Security is of paramount importance to us," he says. "We create, manage and distribute content for the major studios, broadcasters and other content creators, often working on material pre-release."

The CIO of a law firm adds: "A lot of the hackers want the third party data rather than our data. But, hopefully, we are not a soft touch."

Are the systems in your organisation robust enough to withstand attack?

Law firms are less confident about their systems than are respondents outside the law. Only 36% think their systems can withstand attacks compared to 43% in other sectors. Technology firms are particularly optimistic about being able to repel attacks (61%).

Only 24% of legal practices with between 500 and 999 employees think they can see off hackers. By contrast, twice as many (47%) law firms with between 1,000 and 2,499 employees think they should be immune.

Mike Harris, head of policy development at the Institute of Directors, said: "The recent attack on South Korea [when more than 30,000 systems were hacked in March 2013] shows that even the most high-tech economies have vulnerabilities which need to be solved."

Watson says: "You can never be complacent. You must be constantly reviewing and updating your operations."

Many organisations are probably being hacked without them being aware. Anecdotal evidence suggests that the most sophisticated attacks often go undetected for 18 months.

Berman says: "A data breach may go undetected for a very long time. However, once under control, it is important to treat an incident as a starting point in developing greater resilience. This will enable firms to identify and assess the gaps and evaluate the effectiveness of the original plans, procedures and staff training."

Some CIOs are rather sceptical about the solutions being offered to them and the associated cost. One comments: "There is a lot more focus this year on cyber threats. A lot of anti-virus software is based on past viruses. But it is more money [to spend] and is it worth it if it is based on 'what if?'"

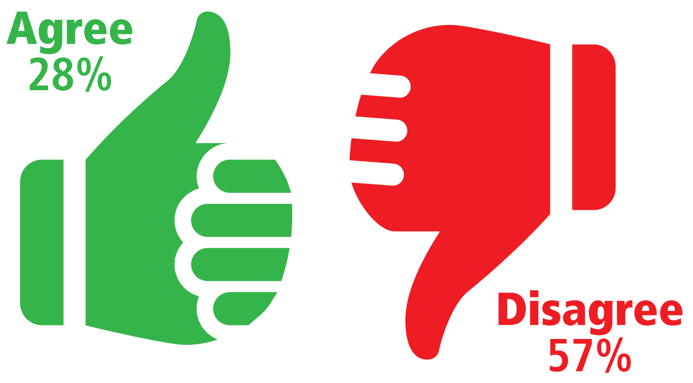
Is your IT team the only group in your organisation charged with repelling cyber threats?

Twice as many organisations (57%) say that the IT team does not have full responsibility for cyber threats as those (28%) which say that the IT function stands alone on this issue. Organisations within the business services sector are more likely (39%) to centralise responsibility with the IT department than those operating in other sectors.

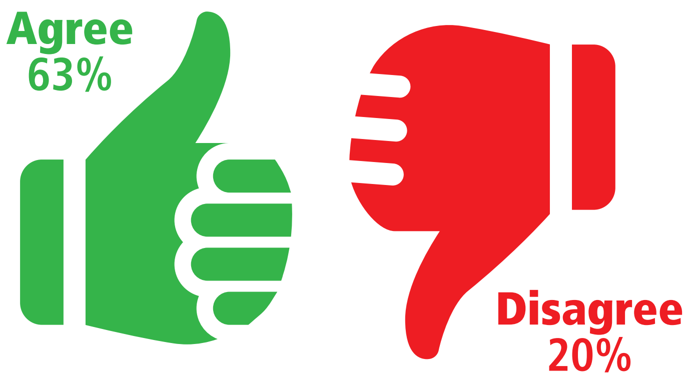
Law firms with turnovers of more

Continued on page 18

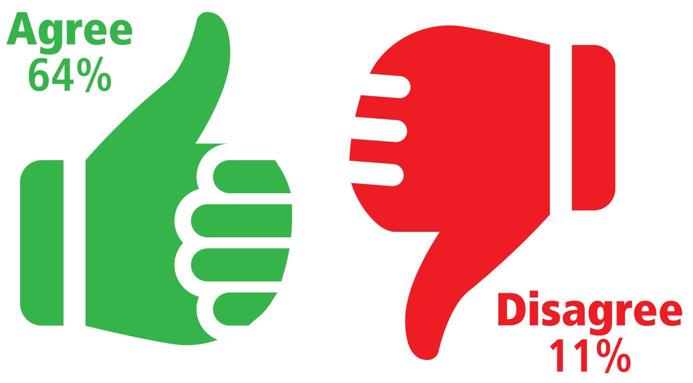
In our organisation, cyber security is the responsibility of the IT operations team alone



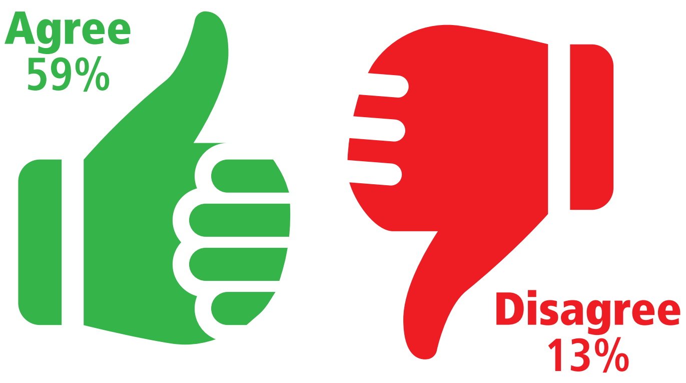
External and internal data security threats are equally prominent



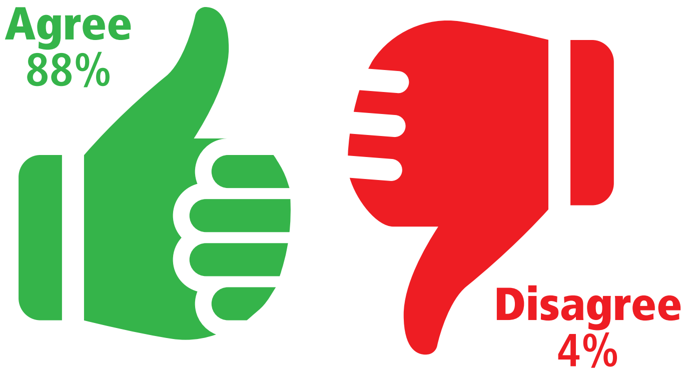
Our business partners take cyber security seriously



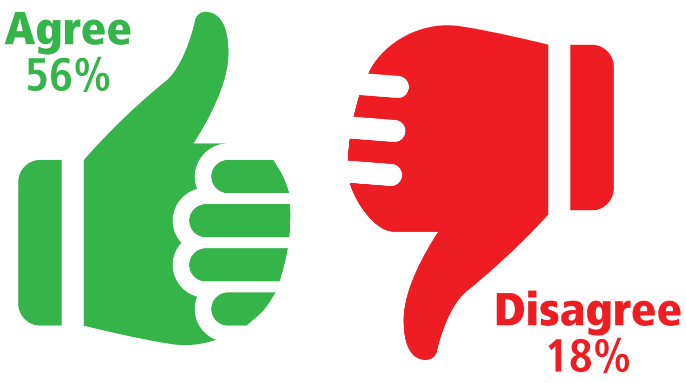
Our organisation would share cyber security threat information with others



Cyber security requires board-level attention



Our organisation has addressed bring-your-own-device security risks



Continued from page 17

than £1bn, are the least likely (6%) to give undivided responsibility to IT teams. The most likely, by turnover analysis, are those with £10m-£50m revenues (37%).

Do you see external and internal cyber threats as being equally important?

Lawyers are slightly more likely (60%) to say that external and internal threats are as much of a threat as each other than people outside law firms (65%).

The smallest law firms by revenue – those with gross incomes of less than £10m – are the most likely to gauge the external and internal threats as being equal (68%). Only 50% of those at the other end of the spectrum – whose revenues exceed £1bn – take the same view.

Nearly eight out of ten (79%) of respondents from technology businesses see external and internal threats equally as much of a threat as each other. Only 44% of business services respondents rate the two threats as being similarly potent.

Do your business partners take cyber security seriously?

Two out of three law firms (62%) think that their business partners take the cyber threat seriously – but this level of trust is slightly higher (66%) among organisations outside the law.

Those working in financial services (75%) and business services (72%) are particularly hopeful about their partners taking the cyber threat seriously. Lawyers (62%) and accountants (60%) are less positive. Firms with 500 to 999 members of staff have more faith in their business partners than those at larger firms, with 76% saying they thought they took cyber security seriously compared to 53% at those firms with between 2,500 and 4,999 employees.

Harris says: “Business leaders increasingly realise the scale and severity of the threat. The task now is to harden our systems before something goes wrong rather than act only in the aftermath of a successful attack.”

Would your organisation information-share with others?

Four times as many (59%) respondents would share information as those (13%) who would not. CIOs (67%) are particularly keen on sharing. Financial services firms (52%) are less willing than lawyers to share data while the technology industry is far more prepared to do so (79%).

The Law Society is encouraging law firms to share information. Setting up a network for this, Law Society chief executive Desmond Hudson said in April: “Firms who work with one another, the Law Society and government agencies will be safer.”

There is also a new Government initiative to encourage industry collaboration called the Cyber Security Information Sharing Partnership (CISP). The head of a small City firm thinks that information-sharing could be difficult to introduce in practice: “It’s extremely difficult to organise. Everybody has an interest in being a free-rider. They would want access to what everybody else knows and then they would only share some of what they know.

“Before people would participate, they’d need to know that there were sanctions as well as carrots. The FBI or whoever it was enforcing it would have to tell them that they would have to participate fully.”

Is cyber security an issue for the top management team?

Nearly nine out of ten respondents (88%) believe that cyber issues require board-level or top management attention. Just 94% of technology entities see cyber security as a boardroom issue.

Among the legal community, 86% agree it is an issue meriting

senior management's attention. In comparison, business services suppliers (78%) are far less convinced.

Nearly all (96%) of law firms with turnover between £100-500m see cyber security as a top management issue. The lowest level of positive response (79%) comes from legal practices with between £10-50m.

Have you addressed the cyber risks of BYOD (bring your own device)?

Law firms (60%) are more likely to have addressed the risks of iPads and other devices owned by their personnel than those outside the law (53%), with the exception of technology companies.

Those in the technology sector (73%) are far more proactive in addressing the BYOD issue, while financial services firms (55%) have lagged behind.

The most active among legal practices, when measured by length of payroll, are those with between 2,500 and 4,999 employees (79%) while the least active are the smallest, with under 100 members of staff (42%).

Has your organisation addressed the cyber risks of the cloud?

Legal practices (51%) are slightly less likely than the average (53%) to have addressed cloud security issues. Technology businesses (73%) and business services organisations (72%) have been actively working to reduce risk on the cloud. Accountancy firms (40%) have been slower off the mark.

When measured by staff numbers, law firms with between 2,500 and 4,999 employees are the most busy (68%) in reducing risks here while those with between 100 and 499 have been the least proactive, with just under half having taken measures to address security.

Dr Stephen Hill is a trustee of the Fraud Advisory Panel, which is supported by the Institute of Chartered Accountants in England and Wales. He says: "Accountants and lawyers will be looking to use the cloud because it's cheaper. If they don't do their homework, however, there are risks about where the data is going.

"Lawyers and accountants often work from client premises, meaning that a cloud-based system becomes very convenient for them to park their data on."

Are UK businesses well-prepared to detect and respond to external cyber attacks?

Nearly four out of 10 (39%) respondents outside of law, and three in 10 (31%) of those in law think that UK businesses are not ready to detect and defend themselves from potential cyber attacks.

Most respondents are unclear on the level of preparedness across UK businesses, with 60% of law firm respondents, and just less than half (48%) of those outside the law, remaining undecided as to whether UK businesses are prepared enough to deal appropriately with cyber attacks.

Few believe that UK businesses are sufficiently prepared, with just 10% of law firms and only 6% of business services enterprises optimistic about their readiness. Technology firms are slightly more optimistic, with 18% thinking that UK firms are well-placed to detect cyber attacks.

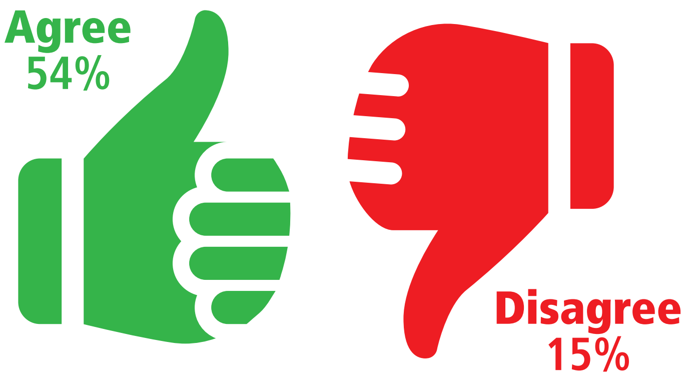
Would your organisation support compulsory reporting of data breaches of personal information?

Partners and staff in law firms are markedly less supportive (53%) of compulsory reporting of data breaches than those outside the legal profession (65%).

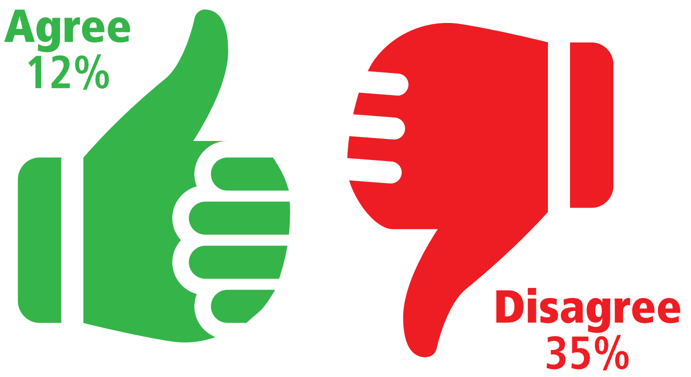
Accountancy practices in particular are extremely supportive of forcing companies to report such data losses, with 80% thinking it should be compulsory.

Continued on page 20

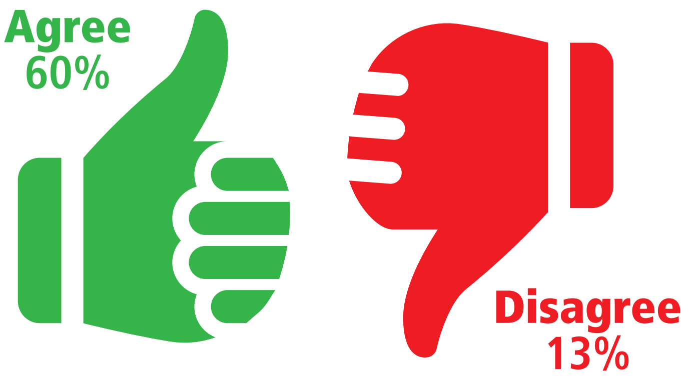
Our organisation has addressed cloud security risks



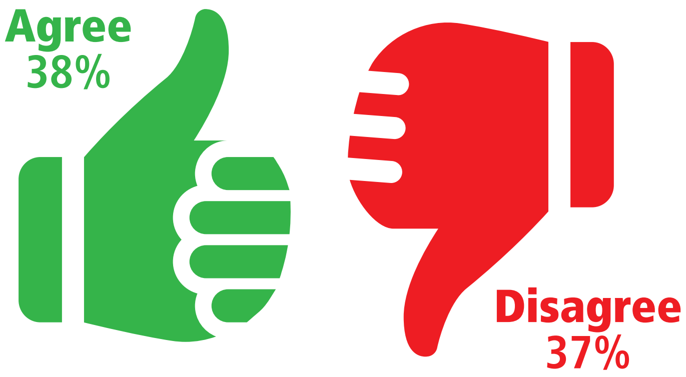
Businesses in the UK are well prepared to detect and respond to external attacks



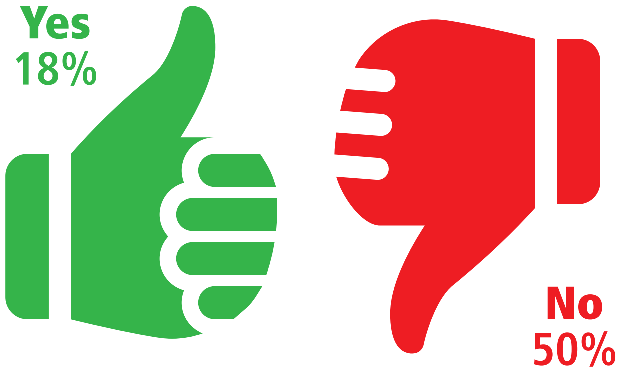
Our organisation would support compulsory reporting of personal info data breaches



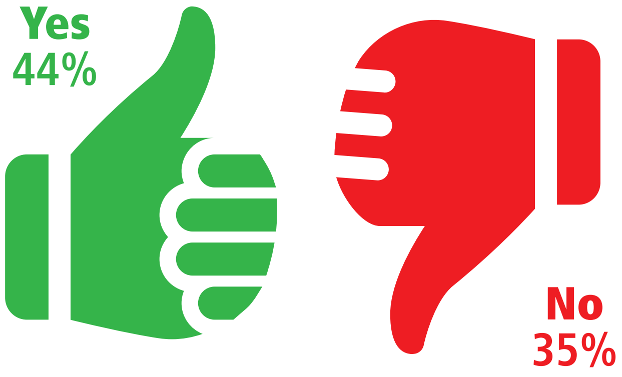
Organisations that invest in IT security are less likely to need cyber insurance



Has your organisation ever been a victim of cyber crime?



Do you have a cyber crime incident response plan?



Continued from page 19

Do you believe that organisations that invest in IT security are less likely to need cyber insurance?

Lawyers are less convinced than those outside law firms that investing in IT security reduces the need for insurance cover. And accountants are less convinced still, with just 20% saying insurance can fall as investment in IT increases. Technology entities have far more faith in IT systems, with almost half (45%) saying better technology requires less insurance.

Does your organisation have a cyber insurance policy?

Insurance policies are not that common in general (17%). but law firms (14%) are less likely to have them than non-lawyers (19%).

Financial services organisations (27%) are nearly twice as likely to have a cyber insurance policy in place than a law firm (14%).

Nearly a quarter of legal practices (24%) with between 500 and 2,499 members of staff have taken out specialist insurance.

If you have insurance in place, what type of event does it cover?

Business interruption (77%) is the most commonly covered event, according to all respondents. This is followed by network security (66%). Business services companies tend to go for insurance policies which cover all the main risks, including cyber extortion and regulatory fines.

By contrast, only 12% of law firms have cover which extends to regulatory fines. Only a third (36%) have opted for cover that covers cyber extortion.

Has your organisation ever been a victim of cyber crime?

Just one in eight (12%) law firms believe their firms have been a victim of a cyber attack. This figure is far lower than those working outside of legal services, where 24% of respondents think their organisation has been attacked.

However, there are twice as many 'don't knows' (44%) among the lawyers than among other respondents (21%), suggesting that it could in fact be rather more than 12% of law firms that have been subject to attack.

In particular, business services firms (39%) and technology companies (24%) are seemingly more frequently attacked, or at least more aware of being attacked.

By number of employees, the law firms which are most subject to attack, or most aware of being attacked, are those with between 100 and 499 personnel (20%). The least likely – or perhaps the least likely to admit it – are those with above 2,500.

Respondents based in the Middle East, Africa and Central America and South America have seen far more attacks than those based elsewhere, with 24% of companies from these regions believing they have been successfully targeted by hackers. This compares to those based in the UK, Europe and Asia where 12%, 18% and 19% respectively have been targeted.

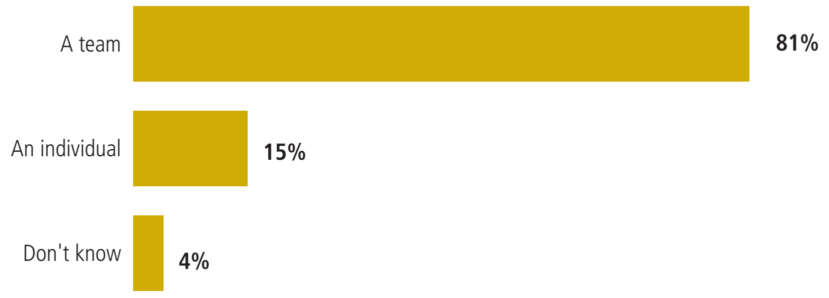
Nearly a third of CIOs (29%) say their organisations have been penetrated by hackers. This falls to 19% among directors and general counsel and to 18% among managing partners.

Do you have a cyber crime incident response plan?

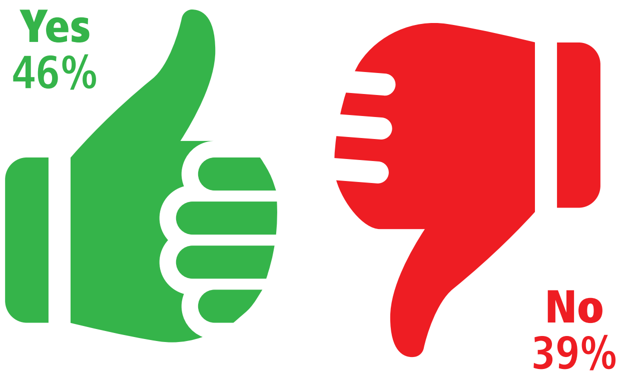
Non-lawyers are far more likely (52%) than law firms (35%) to have a response plan in place for cyber attacks.

Technology firms (64%) and financial services entities (63%) are almost twice as likely as law firms to have a contingency plan in place. Accountancy practices

Is your cyber crime response plan the responsibility of a designated team or an individual?



Does the team include external cyber security specialists?



(60%) and business services organisations (56%) are also markedly ahead.

Nearly two thirds of law firms (58%) with between 2,500 and 9,999 members of staff have a plan in place. At the lower end of the spectrum, only 24% of legal practices with between 100 and 499 employees have an incident response plan prepared.

Stroz Friedberg's Berman says: "Even the best computer security can be breached and firms must be prepared with a response plan in the event of an incident. The first few hours of a data breach are critical and it is too late to think about incident response once security has been compromised."

Contingency plans are seen by experts as being critical in building strong defences against cyber attacks – but these plans are less likely to be found in small professional firms. Hill is most concerned about the firms at the bottom of the range: "In smaller partnerships good governance tends not to be apparent."

If you have a cyber crime incident response plan, is it the responsibility of a team or an individual?

Slightly over four fifths (81%) of all respondents – whether in law firms or not – give the responsibility for producing a cyber crime response plan to a team rather than an individual. Accountants give the responsibility to a team in all cases and business services organisations do so 90% of the time. Technology entities do so in only three quarters of operations (76%).

Teams are favoured by 100% of law firms with between 2,500 and 9,999 employees. But legal practices with less than 100 employees delegate responsibility to teams in only 71% of cases.

As well as having an incident response plan, other measures that firms can take to defend themselves against attack include: having up-to-date network plans, physical access logs, legal notices on log-in, firewalls and training for partners and staff.

If you have a cyber crime incident response plan, does it include external cyber security specialists?

Respondents from the legal sector are less likely (35%) to include external experts in their response plans than respondents outside the legal sector (53%). Business services and accountancy organisations (67% each) are particularly likely to include external cyber security experts.

More than half of law firms with between 5,000 and 9,999 employees (57%) have these outside experts on board. By contrast, only 13% of those with between 500 and 999 staff have nominated these external advisers.

How often do you test your incident response plan?

Partners and employees in law firms (37%) are less likely to know the answer to this question than those working outside the legal sector (23%).

For a quarter of organisations the answer to this question is 'irregularly'. Business services firms test their plans monthly in 30% of cases. This compares to only 12% among legal practices.

But monthly testing increases to 29% among law firms with between 5,000 and 9,999 members of staff. By turnover, monthly testing peaks at 25% for those law firms with revenues of between £50m-£100m.

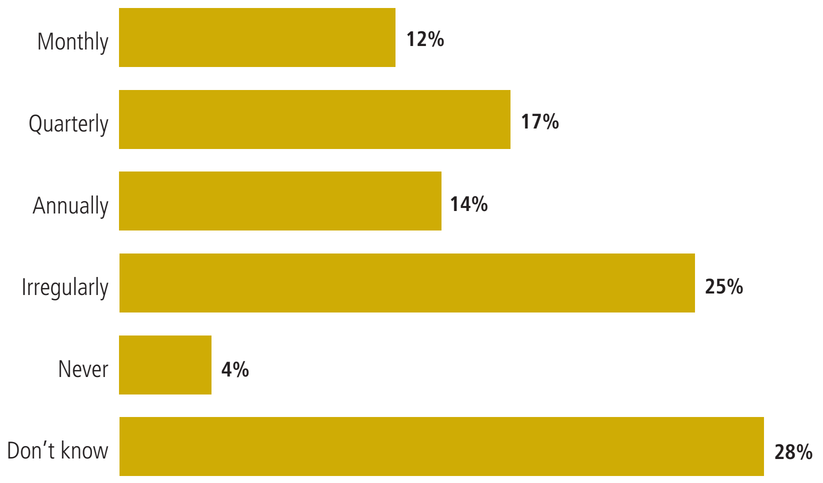
Is the number of threats facing your organisation increasing or decreasing?

Nearly four out of ten (39%) respondents believe that the threats are increasing in number. Only 4% think that the number of threats are falling.

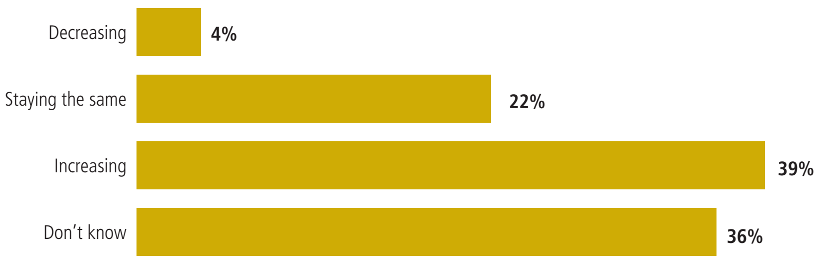
Nearly half of technology enterprises (48%) believe the threat is increasing. Among law firms, when measured by staff numbers, those which are most likely to detect an increase are those with between 5,000 and 9,999 employees (58%). By turnover, the biggest concentration of people

Continued on page 22

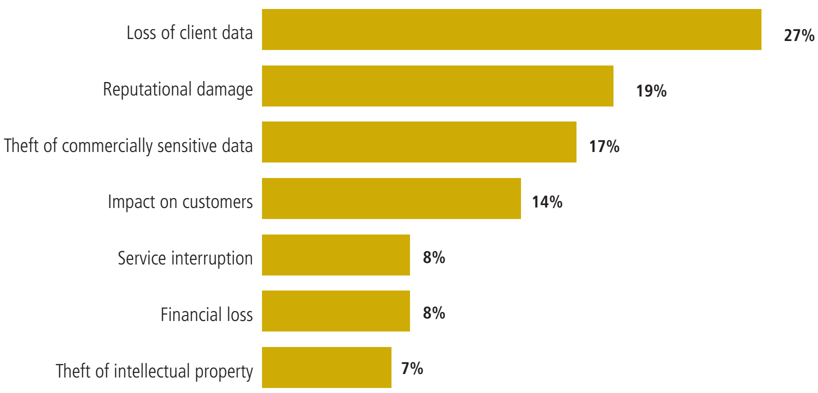
How often do you test your incident response plan/s?



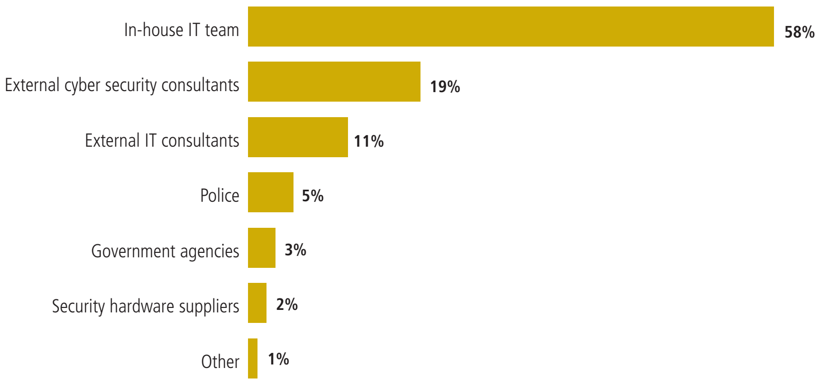
How would you describe the number of cyber threats currently facing your organisation?



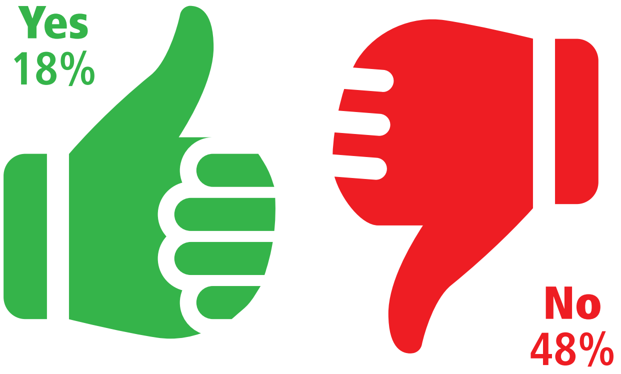
What is your top concern about a cyber attack?



In the event of a cyber attack or data breach, who would you turn to first for assistance?



Has your organisation estimated the potential financial cost of a cyber attack?



Continued from page 21

who see an increase (59%) comes in firms which are bringing in £100m-£500m a year. More than half (55%) of CIOs are seeing an increase, compared to 35% of managing partners.

By geographical region, those in the Middle East and Africa (48%) are most likely to forecast an increase. Those in Central America (38%) and Europe (39%) are at the other end of the spectrum.

Watson says: "Security has improved markedly. However, I suspect that there will be more attacks on law firms in the future and they need to be prepared for this."

What are the top concerns about a cyber attack?

The clearest concern for law firms is the loss of client data (32%). Theft of commercially sensitive data (20%) comes a relatively distant second amongst the legal experts.

Lawyers are twice as worried about theft of commercially sensitive data as are financial services organisations (10%). Service interruption is a much more minor concern for the legal sector (3%) than for, for example, technology operations (18%).

The potential loss of client data is particularly preoccupying for law firms with between 2,500 and 4,999 employees (41%).

Who would your organisation turn to first for help in the event of a cyber attack?

Partners and staff in law firms are more likely to keep the matter in-house, turning to their in-house legal team (in 61% of cases), than those outside the law (56%). The legal profession is also more likely to call in the police (8%) than non-lawyers (3%). In about one in five cases, lawyers (18%) and non-lawyers (20%) would call on external cyber security experts.

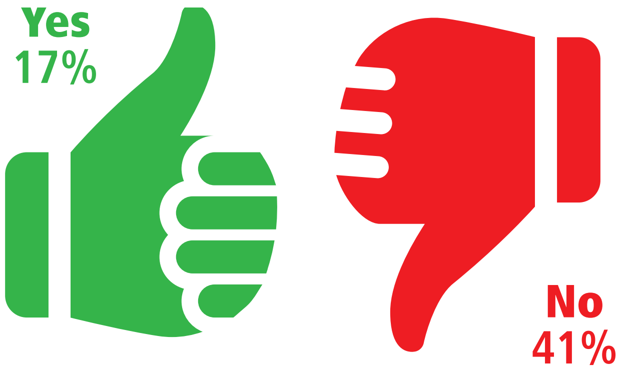
Business services companies (44%) are more than twice as likely as law firms to hire external cyber security experts.

The smallest law firms, those with less than 100 staff, are the most likely to go to cyber experts (23%). Similarly, when measured by turnover, it is the smallest firms (those with revenues below £10m) which are keenest on consulting cyber security specialists (22%).

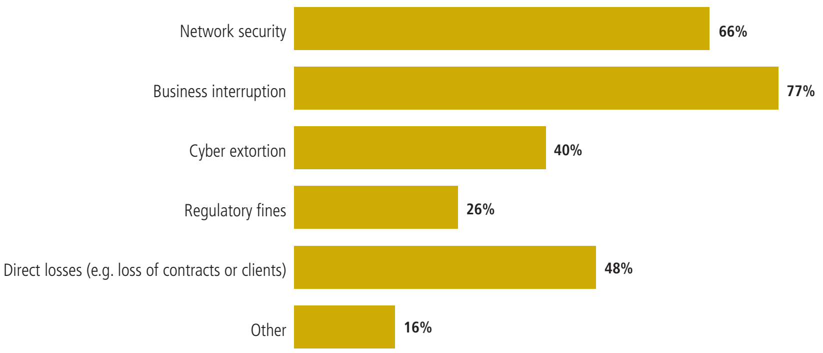
What event or development could raise awareness of cyber security in your organisation?

In nearly two-thirds of cases (61% within the legal profession and 59% outside), a cyber attack that breaches the organisation's

Does your organisation hold a cyber insurance policy?



What type of event does your policy cover?



security would raise awareness. The bitter experience of being hacked is the most effective prompt for raising awareness. Law firms are more likely (45%) to benefit from seeing rivals being attacked than organisations outside the legal sector (36%).

A cyber attack on their own firm would particularly raise awareness in business services companies (72%) but would have far less effect in technology enterprises (52%).

Has your organisation estimated the potential cost of a cyber attack?

Law firms lag behind the rest of the commercial world in terms of estimating costs. Only 9% have worked out potential costs – compared to 26% in businesses outside the legal sector. Another 45% of respondents from law firms do not know if such a calculation has been performed. This means that as many as nine out of ten law firms (91%) may not have gone through the procedure of financial contingency planning.

Technology organisations are more than four times as likely (42%) as law firms to have estimated the likely cost.

Which are the most likely sources to launch a cyber attack?

Criminal gangs (31%) are seen as the most likely attackers among all respondents. Answers here vary little between lawyers and non-lawyers. Hacktivists come second (17%), followed by amateur hackers (16%), competitors (15%), state-sponsored hackers (11%) and, finally, employees (10%).

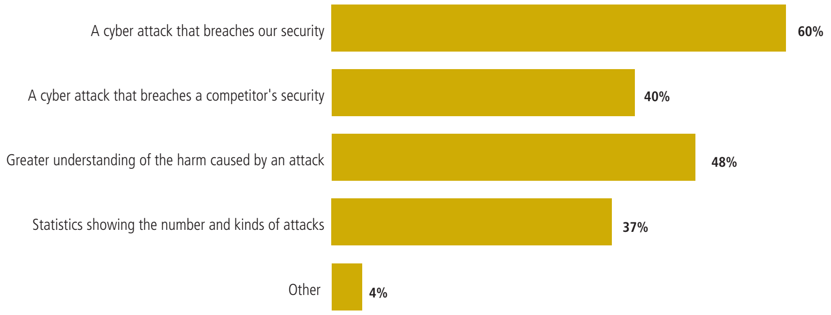
The biggest difference between lawyers and business in general is that lawyers are nearly twice as likely (13%) to suspect employees than those outside the legal profession (7%).

Accountancy firms are twice as fearful (60%) of criminal gangs as law firms are. Technology firms (24%) are markedly more concerned by hacktivists than legal practices are (17%). Technology firms (15%) are also more worried by the prospect of state-sponsored hacking than lawyers are (12%).

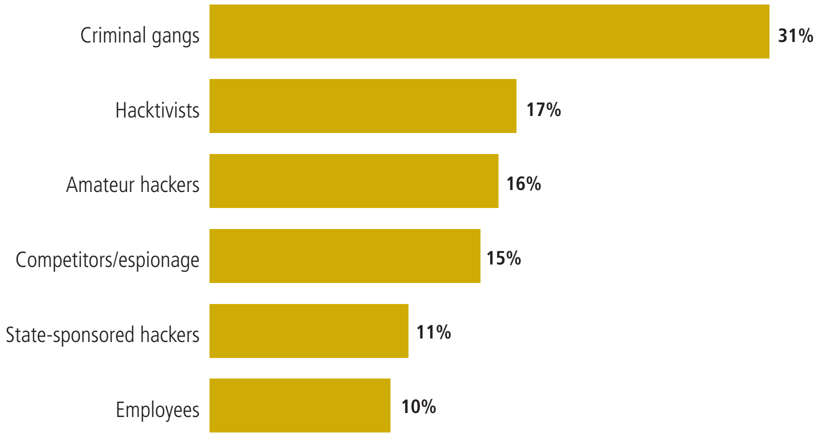
Legal practices with between 5,000 and 9,999 employees are particularly concerned about hacking by state entities (42%).

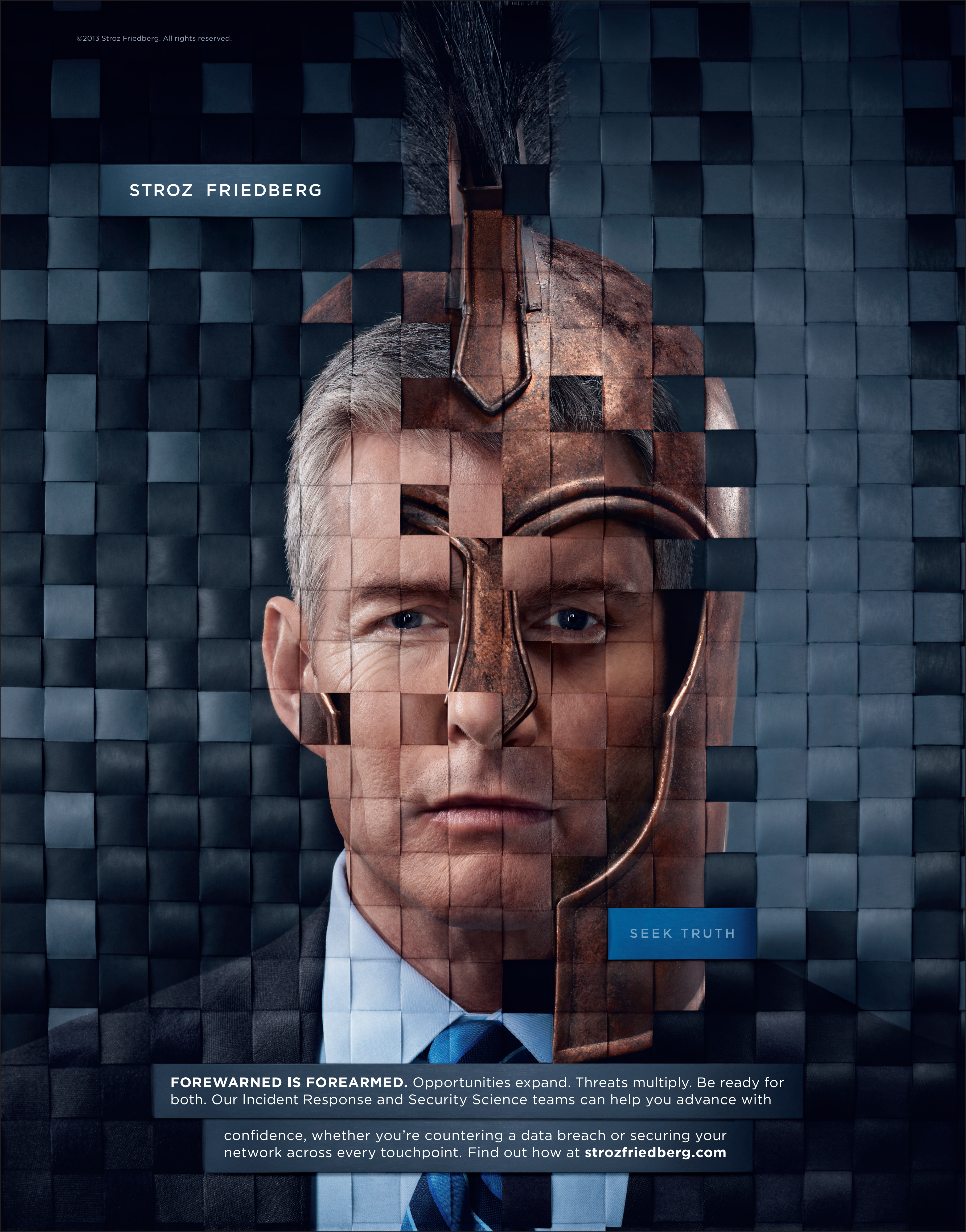
Berman says: “We’re facing an increasingly sophisticated array of adversaries, which makes it important for law firms to recognise the severity of such threats. Phishing emails are becoming increasingly elaborate and are now successfully used to obtain trade secrets, commercially sensitive information and intellectual property.”

What do you believe would significantly raise awareness of cyber security risks within your organisation?



Who are the most likely sources to launch a cyber attack on your business?





FOREWARNED IS FOREARMED. Opportunities expand. Threats multiply. Be ready for both. Our Incident Response and Security Science teams can help you advance with confidence, whether you're countering a data breach or securing your network across every touchpoint. Find out how at **strozfriedberg.com**