The Economist Intelligence Unit

A report from The Economist Intelligence Unit

CYBER INCIDENT RESPONSE

ARE BUSINESS LEADERS READY?

Sponsored by:

ARBOR NETWORKS

Contents

About the report

Cyber incident response: Are business leaders ready? is an Economist Intelligence Unit (EIU) report, sponsored by Arbor Networks. It is intended to gauge the level of corporate preparedness for data-related incidents and examine the level of planning put in place to respond to such an event.

For the purpose of this report we define an incident as any intentional or unintentional breach of a company's security—whether electronic or physical—that materially affects the business. This includes loss of confidentiality (for example, through loss of information), loss of integrity (someone else is in control of processes), and loss of availability (systems outage).

This report draws on two main sources for its research findings.

- In November 2013 the EIU surveyed 360 senior business leaders, the majority of whom (73%) are C-level management or board members. Respondents come from across the world, with 31% based in North America, 36% in Europe and 29% in Asia-Pacific. A total of 19 industries are represented in the survey. Financial services, manufacturing, information technology and professional services are each represented by at least 10% of respondents. Almost half of the companies in the sample (48%) are large organisations, each with an annual revenue of more than US$500m.
- Alongside the survey the EIU conducted a series of in-depth interviews with the following senior executives and experts (listed alphabetically by organisation):
  - Toby Merrill, vice president, professional risk, ACE Group
  - Abbott Martin, senior director, Corporate Executive Board (CEB)
  - Carol Umhoefer, partner, DLA Piper
  - Steve Collins, senior vice president, Edelman
  - Mark Brown, director, cyber security, EY
  - Bob Parisi, practice leader, network security and privacy, Marsh
  - Linda Clark, deputy counsel, data security and information compliance, Reed Elsevier
  - Brad Judy, director, university information systems security, University of Colorado

The report was written by Clint Witchalls and edited by James Chambers. We would like to thank all interviewees and survey respondents for their time and insight.

Executive summary

At the end of 2013, on the busiest shopping day of the year, the US retailer Target was hacked. Early estimates suggested that the hackers stole the payment details of up to 40m credit cards. The number of customers potentially affected was later revised upwards to 110m—around one in every three Americans[1]. A few months earlier Adobe, a US software company, had suffered a similar incident. Initial estimates said 3m customers were affected. The company later updated this figure to close to 40m[2].

Data breaches and denial of service attacks are now so commonplace that only the biggest breaches make the headlines. Yet systems errors and outages are also a major threat. In 2012 the Royal Bank of Scotland (RBS), a UK bank, set aside £125m (US$190m) to cover the costs of a systems outage caused by an error in the bank's batch processing system. Whatever form it takes, the likelihood of a company experiencing an incident is more a question of when, not if.

The costs of these types of incidents, from business disruption to loss of consumer trust, can be significant, particularly for data-intensive industries such as technology, retail and financial services. As such, the ability to manage these situations effectively is both essential and fraught with difficulties. One of the biggest challenges, as these examples demonstrate, is the ability to predict the impact of an incident once it is discovered. So, to what extent are companies prepared for their defences failing or an unforeseen mishap occurring?

Cyber incident response: Are business leaders ready? is an Economist Intelligence Unit (EIU) report sponsored by Arbor Networks. It examines the level of corporate preparedness for data-related incidents and the response plans businesses are putting in place. The report draws on the results of a global survey of 360 senior executives and in-depth interviews with industry experts.

Some of the key findings from the report include the following:

The frequency of incidents is on the rise, but hackers are not always to blame. Over three-quarters of organisations have suffered an incident in the past two years, such as theft of information. The number of incidents is on the increase, although not all are malicious. In the past year, the most common incidents were accidental major systems outages (29%) and the loss of sensitive data by an employee (27%). Therefore, companies should be prepared to respond to a range of potential threats, both external and internal.

[1] http://money.cnn.com/2014/01/10/news/companies/target-hacking/; http://www.nbcbayarea.com/news/national-international/Target-Says-Data-Breach-Affected-70-Million-Shoppers-credit-monitoring-239600681.html

[2] http://www.bbc.co.uk/news/technology-24740873; http://www.telegraph.co.uk/technology/internet-security/10414155/Adobe-hack-affects-38-million-customers.html

The emphasis on incident response is driving the formalisation of plans and processes. With most organisations regularly experiencing an incident, how they respond is becoming an important differentiator. Two-thirds of executives say that responding effectively to an incident can actually enhance their firm's reputation. In light of this, more than 60% organisations now have an incident response team and plan in place. This number is set to rise above 80% in the next few years. Formal plans should retain flexibility, however, since actual incidents rarely conform to prepared scenarios.

Most organisations rely on external providers to assist with an incident response. About 70% of firms—and 80% of large firms—have made arrangements with specialist organisations as part of their incident response plan. The most common standing arrangements are with IT forensic experts or other specialist IT providers, followed by specialist legal advisers. Firms that have suffered an incident in the past two years are twice as likely to have an arrangement with a third-party expert than firms that have not suffered an incident. For now, arrangements with a public relations agency or crisis management firm are less common, underlining the defensive focus of current planning.

The level of preparedness is being held back by a lack of understanding about threats. Nearly three-quarters (73%) of companies feel at least "somewhat prepared" for an incident. Having a formal plan or team in place has a significant effect on the feeling of preparedness among executives. Even so, only 17% of business leaders feel fully prepared for an incident; this falls to 12% in Asia-Pacific. Executives feel least confident about detecting an incident within 24 hours of its occurrence and about their ability to predict its likely impact; greater understanding of potential threats would help them to be better prepared.

Automated detection of incidents is growing in importance, but employees remain vital. Automated detection tools, such as SIEM (security information and event management), detect just over one-third of incidents. In North America, they pick up more incidents than routine checks or controls. Still, employee vigilance is paramount. Globally, employees are most likely to be the first to notify the organisation of an incident. Accordingly, executives and experts recognise the need to raise internal awareness if they are to boost current company preparations.

Firms remain reticent about disclosing incidents and sharing intelligence about threats. The majority (57%) of organisations do not voluntarily report incidents, which they are not legally required to do. This tendency towards secrecy vis-à-vis regulators and the public applies equally to corporate peer groups. While some sectors, such as finance and higher education, collaborate with their competitors to thwart cyber-attacks, the practice is not widespread. Only one firm in three is currently sharing intelligence about threats; this drops to one in four in western Europe.

PLAN OF ACTION

EXPERT ADVICE ABOUT INCIDENT RESPONSE

1. DETERMINE WHAT THE INCIDENT IS

Don't ignore it. "Surprisingly, some people ignore a breach, especially if it appears to be minor. From both a technical and legal point of view, this is extremely dangerous."
Carol Umhoefer, partner, intellectual property and technology group, DLA Piper

Call in the right people. "Ask yourself the question first: could this be a data breach or is this just an operational service issue that we're dealing with? Educate the users not to switch anything off, don't touch anything, but call in specialist assistance."
Mark Brown, director, Cyber Security, EY

2. APPLY THE PLAN TO THE INCIDENT

Think things through before you act. "As soon as you realise you've been breached, you need to assemble the crisis management team and begin to understand the scope of the breach and all relevant facts, including which audiences are affected and what their respective needs and agendas are. The last thing you need is a hasty reaction."
Steve Collins, senior vice president, Edelman

Stick to the plan. "You don't want confusion or panic when an incident occurs, so let each participant fulfil their duties with a capable individual coordinating activity."
Brad Judy, director, university information systems security, University of Colorado

3. COMMUNICATE WITH CAUTION

Communicate. "Remember, security doesn't exist in a bubble. There are various stakeholders within your organisation and outside—plan for their concerns. How will you respond to customers? How can you facilitate transparency? How are internal communications best conveyed: staff meetings, e-mails, or intranet?"
Linda Clark, deputy counsel, data security and information compliance, Reed Elsevier

Be as transparent as possible, but not until you know what you're up against. "One of the biggest challenges facing a firm that has suffered a breach, and the thing they get flak for the most, is how they balance the ever-important considerations of how quickly to respond and how much information to reveal. Coming out too quickly with false information is far more damaging than taking the time to gather the facts and do it properly."
Steve Collins, Edelman

4. REVIEW RESPONSE OUTCOME

Keep an eye on the dialogue. "It's important to monitor the dialogue on the situation, both via traditional news outlets and social media."
Steve Collins, Edelman

Learn from your mistakes. "Every security incident is an opportunity to improve. Improving doesn't mean you've done something wrong, it means you are maturing as an organisation and refining your response."
Linda Clark, Reed Elsevier

Introduction

> “75% of organisations had suffered an incident in the previous two years”

Corporate data and information systems have never been more vulnerable to theft, destruction or denial of access. A survey conducted by The Economist Intelligence Unit and sponsored by Arbor Networks found that more than 75% of organisations had suffered an incident in the previous two years.

Our survey shows that the burden of incidents is spread fairly evenly across regions. Still, industry experts observe underlying trends. Carol Umhoefer, a partner in the intellectual property and technology group at DLA Piper, an Anglo-American law firm, says her company is getting more calls for assistance with data breaches from firms in Asia-Pacific, particularly in Australia, owing to the heightened awareness of privacy obligations in respect of breaches.

Demand for such assistance has remained steady in Europe. In the US, meanwhile, it has been falling. Ms Umhoefer puts this down to the fact that the US pioneered breach-notice requirements. “Most US states have had notice requirements in place for more than five years, and companies are becoming familiar with handling the notice issues,” she says.

Although no industry is left unscathed, some are affected more than others. In our survey, the energy and natural resources sector and the media and entertainment sector both report above-average increases in incidents in the past year.

Mark Brown, director of cyber security at EY, a consultancy firm, says that governments, information technology companies and the oil & gas industry account for the majority of incidents globally. But since these sectors have been under siege for the longest period of time, their information security is relatively mature.

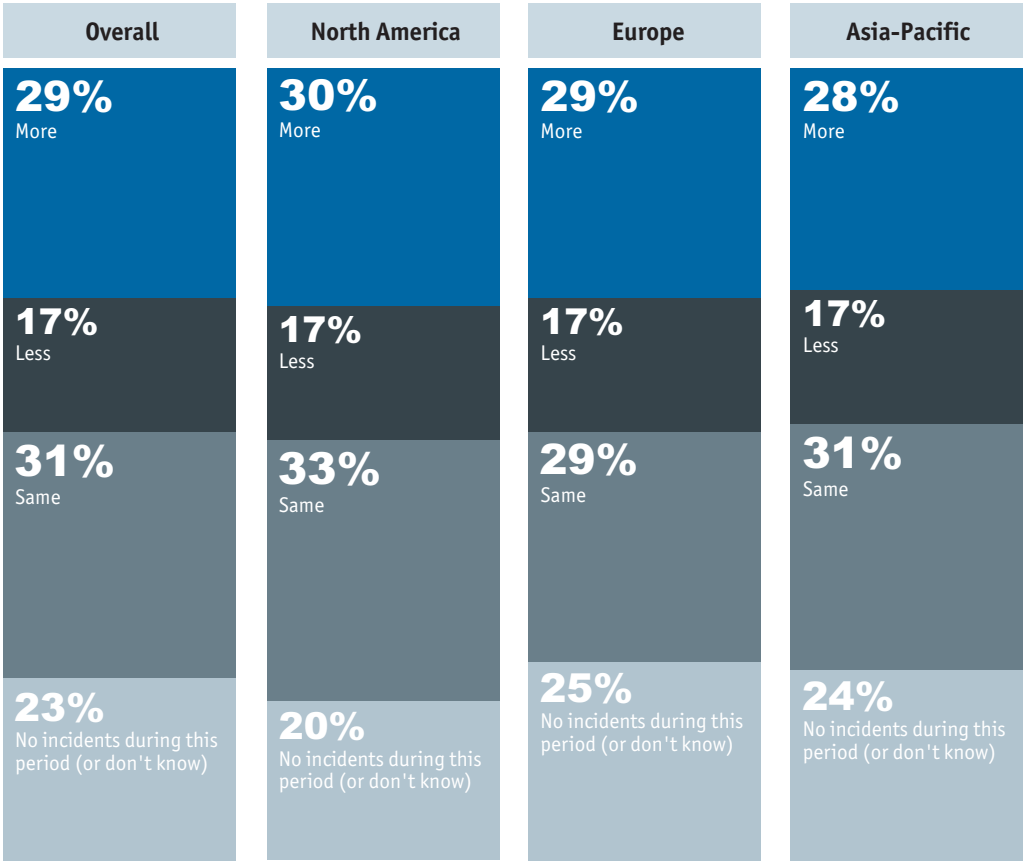
As a result, cyber criminals and “hacktivists” (hackers looking to make an ideological point) are beginning to look elsewhere for weak spots. The media and marketing industries are increasingly being targeted, according to Mr Brown, as they are seen as the “soft underbelly” in the supply chain—a route into more secure industries.

Know your enemy

Understandably, many organisations are focused on thwarting external threats. The existence of state-sponsored attacks to steal intellectual property or trade secrets has been widely publicised, alongside increasingly sophisticated organised crime syndicates. There has also been a surge in hacktivism in the past year, says Mr Brown.

Chart 1: Incident logbook

Incident occurrence: Number of incidents this year compared to last year
(% of respondents)



Incident type: Most common type of incident during last 12 months

1. Accidental major disruption to systems
2. Loss of sensitive data by employee
3. Malicious disruption to systems
4. Theft of sensitive data by employee
5. Theft of intellectual property by employee

Incident detection: Most common method of being alerted to the occurrence of an incident during the last 12 months

=1. Employee
=1. Routine checks or controls
3. Automated detection
4. Customer
5. Supplier

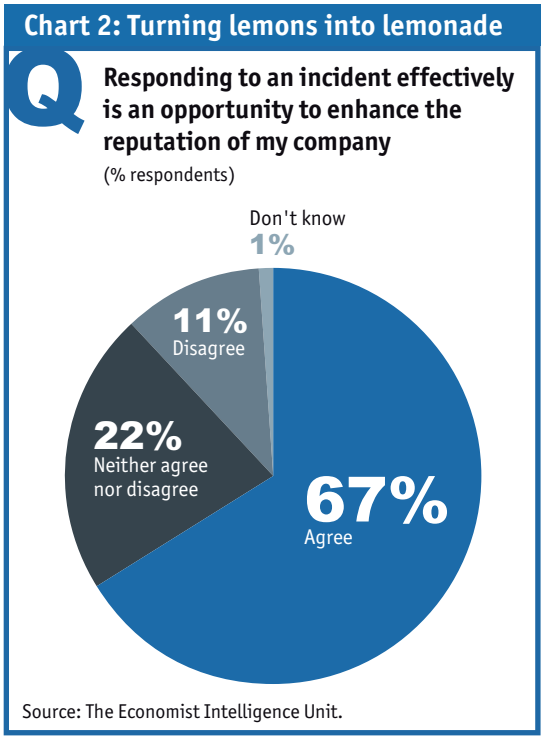
Source: Economist Intelligence Unit.

In 2013 the average cost of cyber crime per US organisations was US$12m—an increase of 26% compared with the average cost reported in 2012, according to the 2013 *Cost of Cyber Crime Study: United States,* published by the Ponemon Institute, a research organisation.

But business leaders should not overlook the internal risks to their company. Often these threats are neither malicious nor deliberate. According to our survey, a company is more likely to lose control of sensitive data through the actions of an employee than as a result of theft by an external actor.

System errors and outages are also a major threat to information integrity and availability, and can be as costly as a data breach. In 2012 the

Chart 2: Turning lemons into lemonade



Source: The Economist Intelligence Unit.

Royal Bank of Scotland (RBS) set aside £125m (US$190m) to cover the costs of a systems outage caused by an error in the bank's batch processing system.[3]

The extent of this risk is borne out by our survey. The most common incidents during the past 12 months were accidental major disruptions to systems, encountered by more than one in four companies (29%).

Given the likelihood of an incident, in whatever shape or form, being prepared to respond is now of the utmost importance. For those companies that get it right, the potential return on investment can be compelling: two-thirds of firms say that responding to an incident effectively is actually an opportunity to enhance the reputation of their organisation.

[3] http://www.information-age.com/it-management/risk-and-compliance/2114773/it-glitch-has-cost-rbs---125m------so-far

1 Plan of attack

> "60% of organisations already have an incident response team and an incident response plan"

It is now commonplace for companies to plan for the event of an incident. More than 60% of organisations in our survey already have an incident response team and an incident response plan. What is more, this number is set to rise above 80% in the next few years as the remaining companies move towards formalising their incident response preparations.

Larger firms (those with an annual revenue in excess of US$500m) are much more likely to have an incident response plan in place than smaller firms with an annual revenue of less than US$500m, but they are catching up: 32% are in the process of putting a plan in place, more than double the figure for large firms.

If and when an incident occurs, the IT function is usually expected to lead the response. This is the case at close to half (49%) of organisations, according to our survey. General management, meanwhile, tends to have direct responsibility at smaller companies, which are less likely to have a stand-alone IT department with sufficient resources and authority. As a result, the calls for more direct senior management involvement are stronger at larger companies.

Alternative scenario

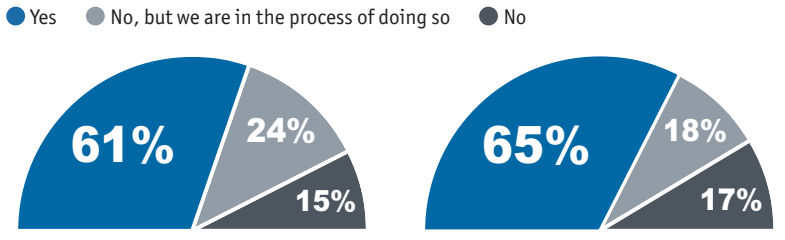
Many organisations have plans in place to respond to specific scenarios. For instance, they have a response to a data breach, a hacktivist attack or a password loss, among many others. According to our survey, close to one-half of companies have a formal method for classifying an incident as soon as it is detected.

This move towards a formalised response plan comes with a note of caution, however. Some experts emphasise the need to retain flexibility within these processes. The most likely scenario is that when an incident occurs, it will not fit neatly into the plan.

What companies should be developing, therefore, is a response capability. Incident response teams and plans should identify the right people to bring together to react to the situation in hand and respond accordingly. This can often mean

Chart 3: Be prepared

Formal response preparations
(% of respondents)



Source: Economist Intelligence Unit.

recognising the limitations of the company's resources and drawing on external support.

At Reed Elsevier, a media organisation, the incident response team includes security experts, auditors, investigators and in-house counsel. Linda Clark, the firm's deputy counsel for data security and information compliance, says that if necessary, the company also brings in additional expertise. "What is needed depends on the specific threat being examined," says Ms Clark. "You might decide that you need involvement from finance, product development, engineering, or outside consultants."

Indeed, about 70% of the firms surveyed—and 80% of the large firms—have made arrangements with specialist organisations as part of their incident response plan. Having an arrangement with third-party experts is twice as likely at firms that have suffered an incident in the past two years than at firms that have not.

IT forensic experts or other specialist IT providers are most likely to be called on for assistance, followed by specialist legal advisers and law enforcement. By contrast, arrangements with external public relations firms and crisis management providers are much less common.

"Typically, the moment a company has a breach they will start asking for support, because very few companies have this in-house capability to do the full and true forensic analysis and evidence gathering," says Mr Brown of EY, who draws a direct link between forensic and legal expertise. "It's a very litigious process. If you are looking to be able to prosecute the perpetrators at the end of a breach, you need to be able to preserve the evidence. In addition, you need to be able to collect the evidence in such a way that you truly know what the breach was and how it occurred."

Often, the need to get a system operational again can outweigh the need to investigate what actually happened. But it is important to treat an incident as though it were crime scene, and that means not touching anything.

Safety net

In recognition of the heightened risk, a growing number of companies are taking out insurance policies to cover specifically against cyber-related incidents. Marsh, a global insurance broker, saw demand from its US corporate clients increase by one-third between 2011 and 2012. Bob Parisi, the company's network security and privacy practice leader, has seen the trend continuing in 2013 and expects it to continue into 2014. A variety of factors are behind this uptick, including regulatory changes, contractual requirements for coverage, media reports of data breaches, and actual experiences of a breach.

This trend, initially led by larger organisations in the US, is now being driven by mid-market companies with annual revenue between US$50m and US$1bn, according to Toby Merrill, vice president for professional risk at the insurer ACE Group. To meet the needs of this market, where companies typically have fewer resources in-house, insurers such as ACE offer additional services. These include a suite of approved vendors to use, such as IT forensic experts and call centres to handle customer enquiries and complaints.

As is to be expected, interest in privacy cover is strong among industries dealing with a lot of personal data, such as retail, healthcare, financial services and education. The costs of losing personal data are readily quantifiable by reference to regulatory fines. There is also the likelihood of litigation. According to Mr Parisi, most US companies disclosing the loss of personal information can now expect to be subject to a class action lawsuit—even when that data loss did not result in any financial damage.

Nonetheless, other industries with fewer privacy concerns are showing greater interest. In manufacturing, for instance, IT systems and technology have become so integral to the manufacturing process—right across the supply chain—that business executives are realising what an interruption in these systems could

mean for their business. There will also be a rise of business-to-business (B2B) litigation between companies, according to Mr Merrill, as more companies are under a contractual obligation to notify partners about breaches.

Still, widespread coverage across industries is a long way off. Mr Parisi puts the market penetration rate for these cyber insurance products at around 25% in the US and in single digits everywhere else.

Outsourcing risk

Preparations should not be limited to incidents directly affecting the company, however. According to Mr Merrill, one incident in three is caused by a third-party business, but current incident response planning is not paying sufficient regard to the implications of this.

The growth of outsourcing, from customer services to data storage, has exposed companies to greater risk of incidents involving their data, which they may have failed to fully appreciate when the initial contract was signed. Most aspects of dealing with an incident, from detection through to employing a forensic team to examine the compromised computer systems and notifying affected parties, become more complicated when it involves the network systems of a business partner, such as a supplier, or a service provider, such as a cloud storage provider.

Accordingly, Mr Merrill suggests that companies check their contracts with key suppliers and vendors to see what the obligations are. In our survey, one half (51%) of respondents believe their major partners, such as suppliers and vendors, would immediately notify them of an incident that might affect their company, although a sizeable minority (29%) are either undecided or don't know.

For now, the majority of business leaders appear sanguine about these risks: only around one-third (31%) believe that closer integration with other companies has made it more difficult to co-ordinate their company's response to an incident. But again, this can be partly explained by a lack of information. More than one-third (36%) of executives are either undecided on this point or do not know enough to give a definitive answer.

Going public: A long-term investment

January 20th 2009 was an important date. It was the inauguration of America's first black president, Barack Obama. It was also the day on which Heartland Payment Systems announced that its systems had been breached. Critics accused Heartland of using the auspicious date to try and bury bad news.[4]

But if that was the US-based payment processing firm's intention, it failed. Within days of the announcement, Heartland's share price fell by 50% and continued its sharp descent into early March 2009, losing 78% of its pre-breach value at its lowest ebb.

Even when sensitive data are not stolen, a data breach can have an impact on share price, as Sony learned after its European subsidiary's websites were breached in June 2011. The data that were stolen were already in the public domain, but that did not stop 2% being knocked off the firm's share price.[5]

Although data breaches are common, protecting data is important if an organisation wishes to maintain the trust of its customers, investors and other stakeholders. If a data breach breaks this trust, it can have a significant impact on share price, says Abbott Martin, senior director at Corporate Executive Board (CEB), a business advisory firm. But Mr Martin admits that the impact of an incident on share price is "difficult to quantify".

One lesson that can be learned from the Heartland incident is that being open about a data breach is not detrimental in the long run. Heartland's chief executive, Robert Carr, tried to be as open as possible about the breach and encouraged other firms to share information about cyber-attacks. He also co-founded the Payments Processing Information Sharing Council (PPISC), an organisation that encourages firms in the payments industry to exchange relevant information.

If Heartland's share price took a plunge after the breach announcement, it has certainly rallied since then. On March 9th 2009, less than two months after the event, Heartland's share price opened trading at US$3.98. By 2013 its shares were trading at more than ten times that value.

[4] http://www.businessweek.com/stories/2009-07-06/lessons-from-the-data-breach-at-heartlandbusinessweek-business-news-stock-market-and-financial-advice

[5] http://www.computerweekly.com/news/1280096016/Sony-hacks-hit-share-price-in-Tokyo-as-data-breaches-undermine-confidence

2 Preparing for the unknown

> “Only 17% of executives feel fully prepared…”

Senior business leaders are reasonably confident of their company’s ability to respond to an incident. Nearly three-quarters (73%) of respondents to our survey feel at least somewhat prepared for an imminent incident affecting their company.

The influence of formal preparations on this business confidence is clear: over 90% of companies with an incident response plan or an incident response team feel prepared for an incident, compared with just over one-third of companies with no such formal procedures in place. There remains significant room for improvement, however, since only 17% of executives feel fully prepared; this share drops to a regional low of 12% in Asia-Pacific.

Once plans are put in place, they should be tested and updated on a regular basis. Although a company may have robust preparations in place, the implementation of an incident response plan will ultimately depend on the culture of the organisation, says Mr Merrill of ACE Group, particularly the personalities involved. Moreover, the nature of the threats to a company is constantly changing, so plans should be updated and tested to take account of these developments.

Reports on the frequency of such tests are mixed, however. According to Mr Merrill, testing is not as common as it should be. Meanwhile, Mr Parisi of Marsh reckons nearly all of the companies he works with regularly conduct a so-called “table-top” test of their incident response procedures, certainly on an annual basis, or even month to month. This group is fairly representative of the US economy, he says, although other countries are not so far along. Some industries, moreover, are conducting such exercises on a much larger scale.

Knowledge is power

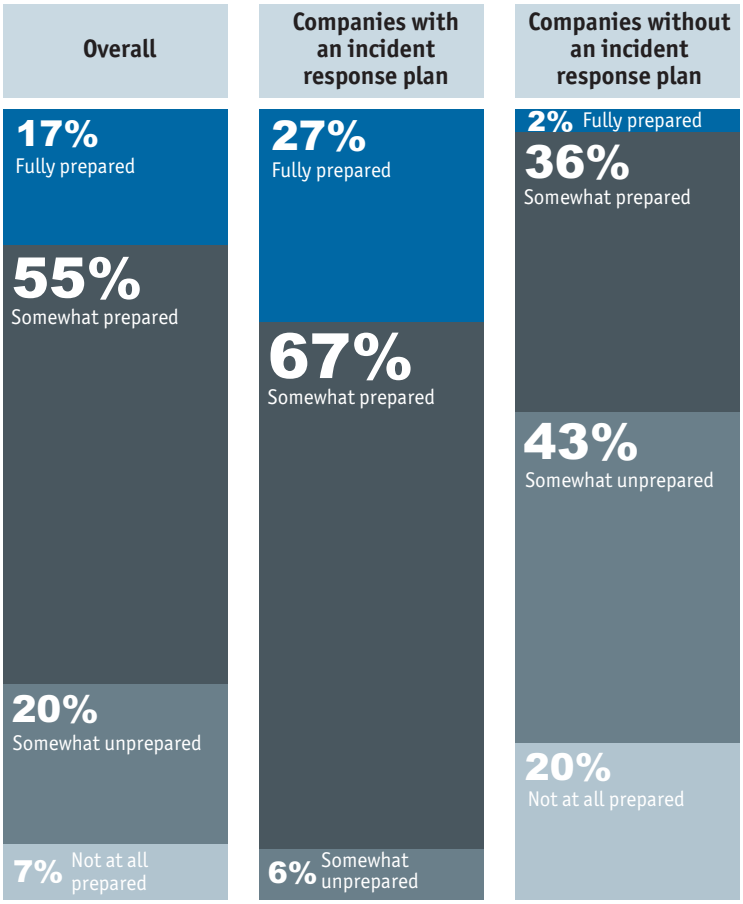
Education is another, more pressing need, according to experts and executives. Nearly one in three business leaders in our survey believe that their organisation would be better prepared if they could raise awareness of existing incident response preparations across the company.

For Brad Judy, the director of university information systems security at the University of Colorado, an effective response plan has to be both well defined and well communicated. Companies should, therefore, ensure that those responsible for implementing response plans are empowered to educate the organisation about those plans, which may not always be the case.

The importance of raising awareness and education is underlined by the detection of incidents. Our survey shows that in 46% of

Chart 4: Quietly confident

Q **Readiness level: How prepared would your company be to respond if it discovered an incident tomorrow?**
(% of respondents)



Raising the standard: What would assist your company to be better prepared for an incident?

Top 3 responses

1. Better understanding of the potential threats to my company
2. Raising awareness of existing preparations across the company
3. Testing existing preparations for an incident

Potential weak spots : Where are you the least confident about your company's ability to respond to an incident?

Top 3 responses

1. Accurately predict potential business impact
2. Discover the incident within 24 hours of it occurring
3. Manage media reporting of the incident

Source: The Economist Intelligence Unit.

and routine checks. To a certain extent, elevated employee awareness can even explain the rising number of incidents reported by companies: simply being better able to recognise an incident means an employee is more likely to report it to the relevant department.

Automated detection systems, such as SIEM (security information and event management) and IDS (intrusion detection systems), also play an important role. Just over one-third of known incidents are picked up by these automated detection tools. In North America, automated detection tools are picking up more incidents than routine checks or controls.

Yet, as useful as these tools are proving to be, they can be a double-edged sword. "The same information security tools are available to cyber criminals to exploit systems," says Mr Brown of EY. "The difference is that cyber criminals are able to move at a pace that far outstrips the pace of a legitimate business." An organisation will have a procurement cycle, but a criminal can just log onto a website and order the latest tools using a stolen credit card.

Strength in numbers

More than anything else, senior executives believe that an increased understanding of the potential threats to their company would help them to be more prepared. Lacking an accurate picture of the types of threats to their company understandably makes it difficult for them to prepare fully to respond. These knowledge gaps, or "known unknowns", are unnerving for business leaders, who lack confidence in their company's ability to predict the business impact of an incident.

This may be because many incidents are what Nassim Nicholas Taleb, an academic and author, calls "black swan events"—events that deviate from the norm and are hard to predict.[6] Not surprisingly, having an incident response plan in place and a team to carry it out seems to do little to boost confidence in this regard.

[6] Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable*, Penguin, 2008.

cases it is an employee who first notifies the organisation of an incident. Indeed, employee notification appears to be as effective as controls

Understanding the nature of the threats is hard, given that they are constantly, and often rapidly, evolving. Over the past three years Ms Umhoefer of DLA Piper has seen a marked increase in advanced persistent threat (APT) attacks—attacks that are highly sophisticated, hard to detect and often state-sponsored.

"There has also been a more gentle evolution from smaller, accidental breaches, such as lost back-up tapes, to more systematic, industrial and bigger cyber-attacks, including capturing data or devices and issuing ransom notes," says Ms Umhoefer.

Sharing intelligence on threats with competitors and industry groups would go some way towards raising awareness of these new types of threat. Information security professionals believe that closer co-operation between companies is the only way to tackle the problem.[7] But progress here is patchy.

About one in three firms share information about incidents with other firms in their industry. North American firms are once again leading the way. Some sectors, moreover, are particularly active in this regard. In November 2013 a number of financial services firms, infrastructure providers and financial authorities banded together to run a simulation of a cyber-attack on London's financial centre.[8]

The purpose of the exercise, called Waking Shark II, was not to test the robustness of individual firm's response plans, but to identify "co-ordination issues in the event of a major attack". Firms on Wall Street have run a similar simulation called Quantum Dawn.

The higher education sector in the US also has a history of collaboration when it comes to cyber security. "Sharing information is one of the strengths of information security in the higher education industry, and we use multiple methods to share information and collaborate," says Mr Judy of Colorado University.

Damned if you do, damned if you don't

Possibly because of the stealthy nature of many attacks (especially APTs), more than one in three respondents lack confidence in their ability to spot an incident within 24 hours of its occurrence.

"The likelihood that you will know about an incident having occurred within 24 hours is minimal," says Mr Brown of EY. "Even if you do, the likelihood that you would actually know the full details of what had happened in 24 hours is even more minimal."

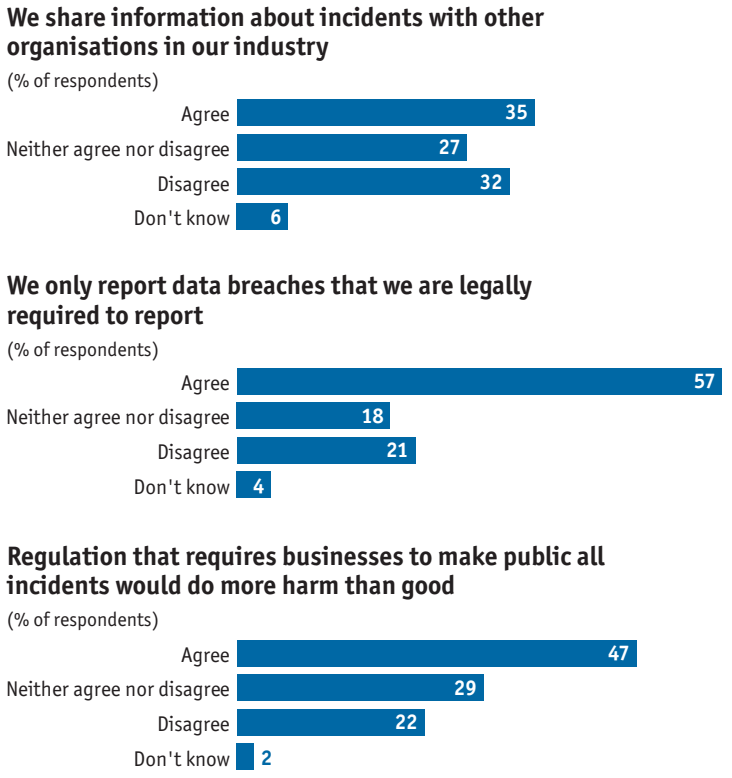
Indeed, the time it takes to detect a breach may be getting longer. According to a report from Trustwave, an information security company,[9] it took businesses 210 days on average to detect a breach in 2012, an increase of 35 days on the equivalent figure for 2011.

[7] http://www.scmagazine.com/rsa-conference-2012-cyber-crimes-biggest-enemy-is-collaboration/article/230377/

[8] http://www.bankofengland.co.uk/financialstability/fsc/Documents/DesktopCyberExercise(WakingShark).pdf

[9] http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf

Chart 5: Open data



Source: Economist Intelligence Unit.

Against this backdrop, the ability of companies to predict the impact of a breach and detect it within 24 hours of it occurring looks set to come into greater focus as governments across the world move towards making breach notifications mandatory. According to Mr Brown, many of EY's Europe-based clients are concerned about the impact of new EU legislation, which will make it mandatory to notify national authorities of a breach within 24 hours of it occurring.[10]

While Mr Brown is in favour of mandatory reporting, he would prefer the ruling to change so that reporting to the authorities is only done after the organisation has identified the full extent of what has happened. "Are companies able to know what's happened?" he asks. "Not always. Are they able to report in such a short period of time what's happened? Almost never."

Selective disclosure

Reporting the loss of personally identifiable information (PII) to regulatory authorities is mandatory in many countries, but should firms consider reporting incidents that do not involve a loss of PII, such as the loss of trade secrets or information about a confidential business deal?

The University of Colorado has an official process to report any major security incidents to the Colorado Department of Education, whether or not it involves breaches of personal information. Yet this practice is a minority position among companies. For now, a simple majority (57%) of organisations only report data breaches if they are legally required to do so (a further 22% are ambivalent or undecided).

In keeping with this viewpoint, there is little support for regulation that would require businesses to make all incidents public. The largest group of executives (47%) believes this would do more harm than good—more than twice as many as those who take the opposite view (22%). But here again, a sizeable contingent (29%) are undecided about whether it is a good idea or not.

With the increased focus on incidents and the push among rulemakers for greater transparency, executives would be wise to prepare for this eventuality. The Securities and Exchange Commission (SEC), for example, already requires US publicly listed companies to disclose all material events in their regulatory filings, including data breaches.

While declaring a breach can cause damage to a business in the short term, it can be more damaging if it is later revealed in the press that there was an incident but the organisation decided not to report it. What is more, keeping incidents secret is getting harder, given the ubiquity of technologies such as social media.

The challenge for regulators is to reach a workable solution that allows companies to disclose this information without being unfairly compromised. Regulators need also consider their own capacity for this move. In 2012 the UK's Information Commissioner, Christopher Graham, encouraged rulemakers to continue with an element of selective disclosure[11], fearing that the introduction of mandatory data breach notification requirements would bury his office under a deluge of paperwork. As with most elements of incident response, an element of flexibility is called for.

[10] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[11] http://www.computerweekly.com/news/2240203760/EU-data-breach-disclosures-to-be-enforced-soon

Conclusion

Over the next few years the readiness of businesses to respond to incidents will grow. Whether it is an advanced persistent threat or an employee losing a client list, most organisations now have an incident response plan and a team to cover it. These preparations are being tested and developed, and specialist external assistance is added when and where required.

But even with these measures in place, senior business leaders have lingering doubts. Chief among these are the ability to predict the potential business impact of an incident and the capacity to identify an incident within 24 hours of its occurrence. These business leaders would feel better prepared if they had a greater understanding of the potential threats facing their organisation.

Learning how peers and competitors have dealt with an incident—through sharing information and industry-wide testing, rather than waiting for an actual incident to happen—is one way to benchmark a company's existing preparations. While security professionals are showing willingness, C-level executives still need to be convinced.

At the same time, executives should not overlook the internal risks from accidental systems outages, the loss of sensitive information or the crucial role of employees in the detection process. The need to raise awareness across the company has been identified. Now it is for business leaders to put this realisation into practice.

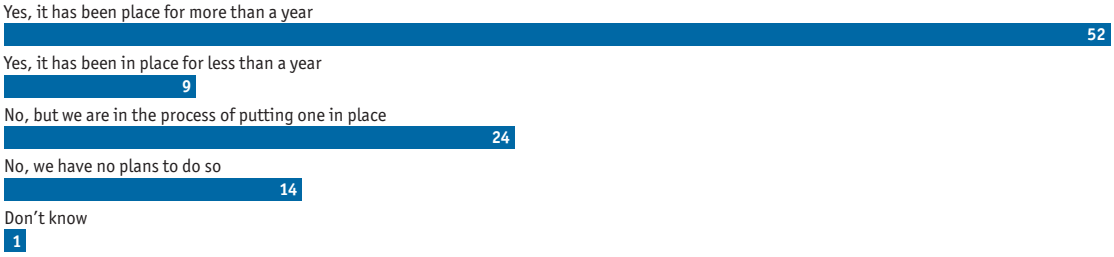
Looking further ahead, companies should be prepared for every major incident entering the public realm. Many countries have made it a legal requirement to report data breaches, especially if they involve personally identifiable information. But even when mandatory reporting is not required, news often leaks out via social media.

Suffering some sort of incident is now seen as more of a fact of doing business than a sign of ineptitude. In this environment, the emphasis on a defensive, IT-led response needs to evolve into more active management and communication. Ultimately, the way in which companies respond to these incidents is how they will be judged.

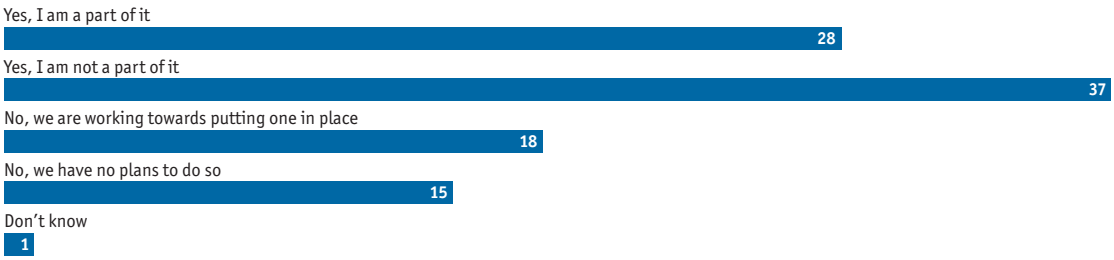
Appendix: Survey results

In November 2013 The Economist Intelligence Unit conducted a global survey of 360 senior business leaders. All of the questions asked in this survey are included below. Please note that not all answers add up to 100%, either because of rounding or because respondents were able to provide multiple answers to some questions.

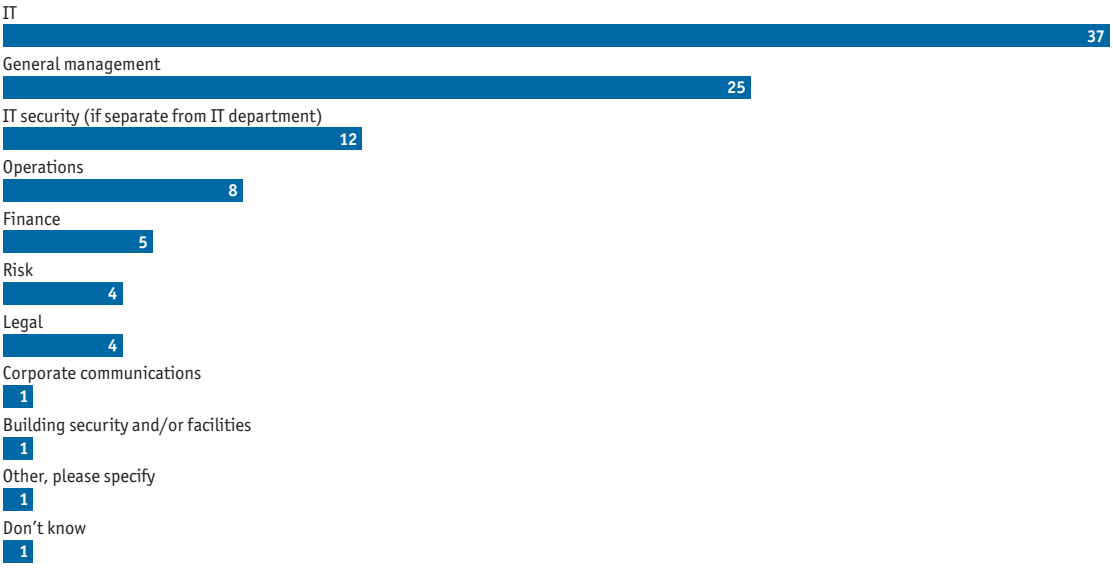
Does your company have a formal incident response plan in place?
(% respondents)



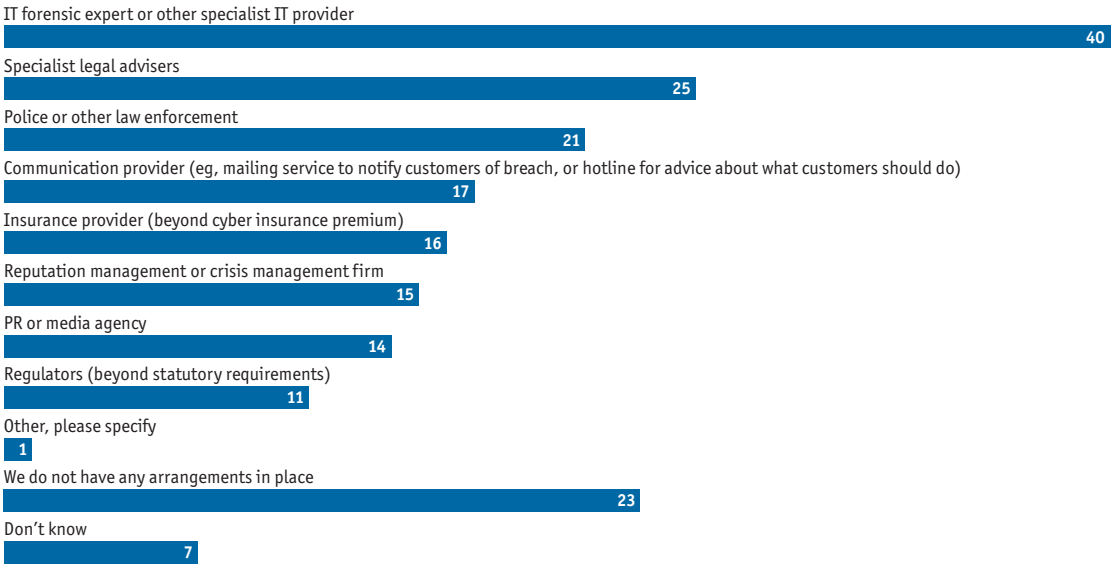
Does your company have an incident response team?
(% respondents)



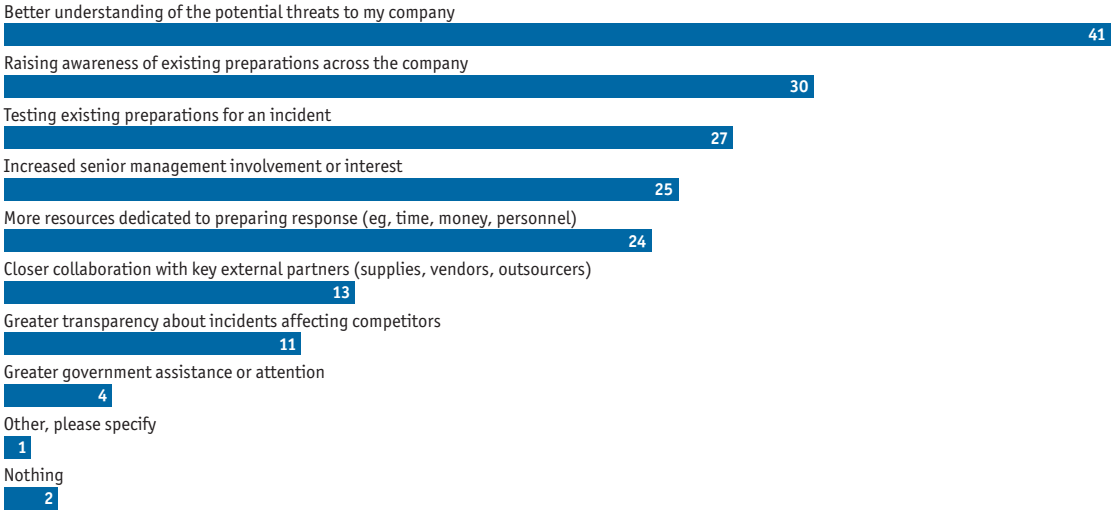
What department or function leads your company's response to an incident?
(% respondents)



Has your company made arrangements with any of the following organisations as part of its incident response plans or preparations? Select all that apply
(% respondents)

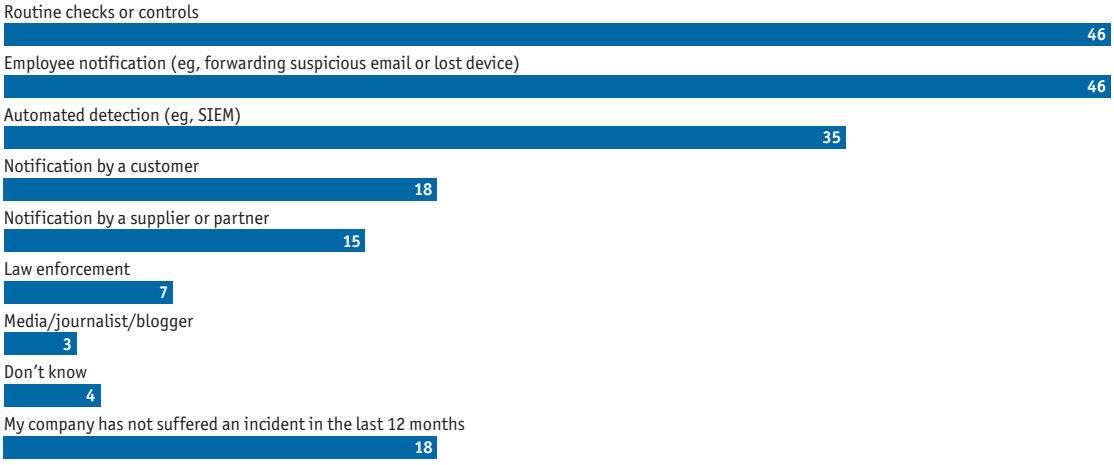


What would assist your company to be better prepared for an incident? Select up to two
(% respondents)



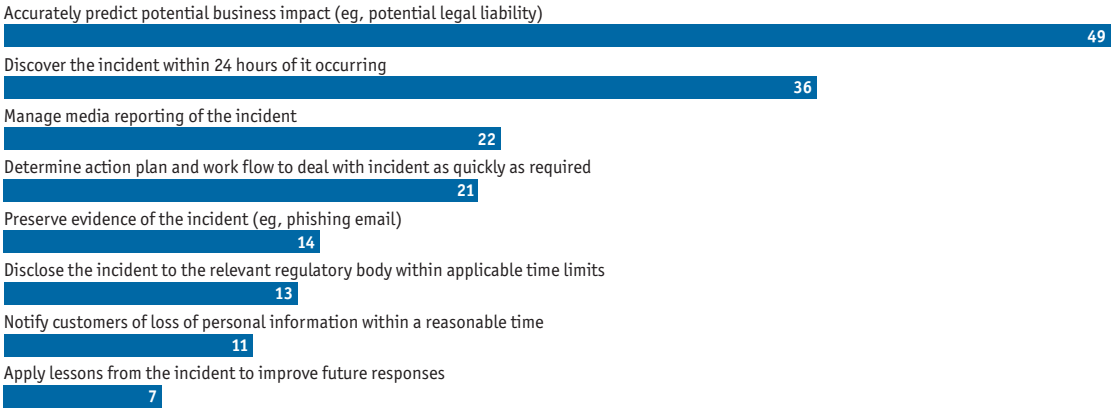
How prepared would your company be to respond if it discovered an incident tomorrow?
(% respondents)

How has your company been alerted to the occurrence of an incident during the last 12 months? Select the three most common, if applicable
(% respondents)



To what extent do you agree or disagree with the following statements? Select one column in each row
(% respondents)

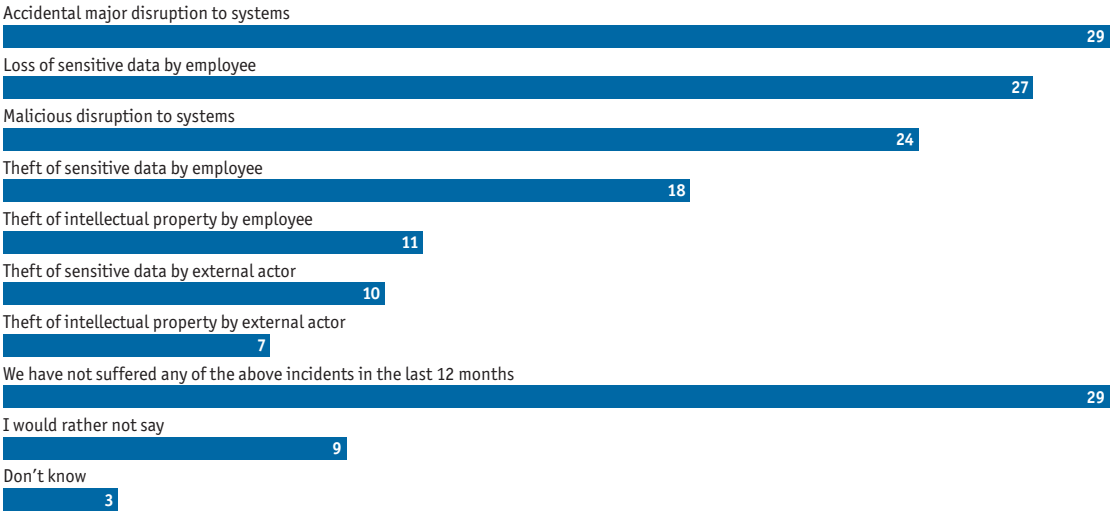
In which of the following areas are you the least confident about your company's ability to respond to an incident?
Select up to two
(% respondents)



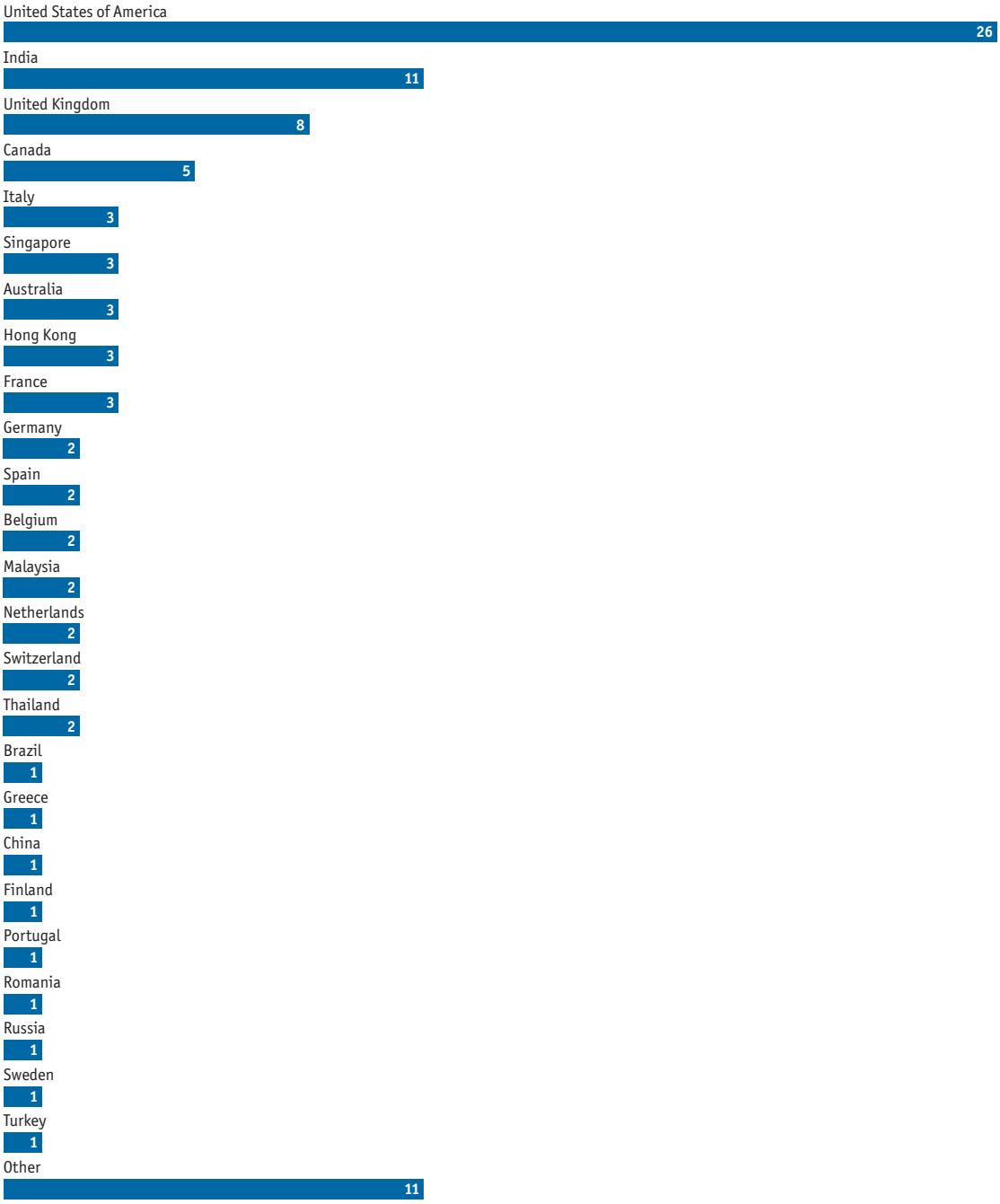
To what extent do you agree or disagree with the following statements? Select one column in each row
(% respondents)

Roughly how many incidents has your company experienced this year compared to the same period last year?
(% respondents)

To the best of your knowledge, which of the following categories of incident has your company experienced at least once over the last 12 months? Select all that apply
(% respondents)

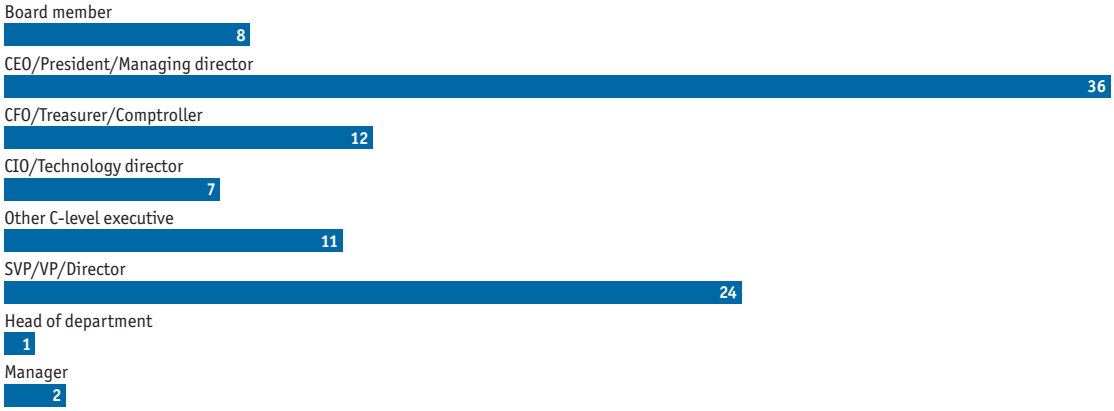


Where are you personally located?
(% respondents)

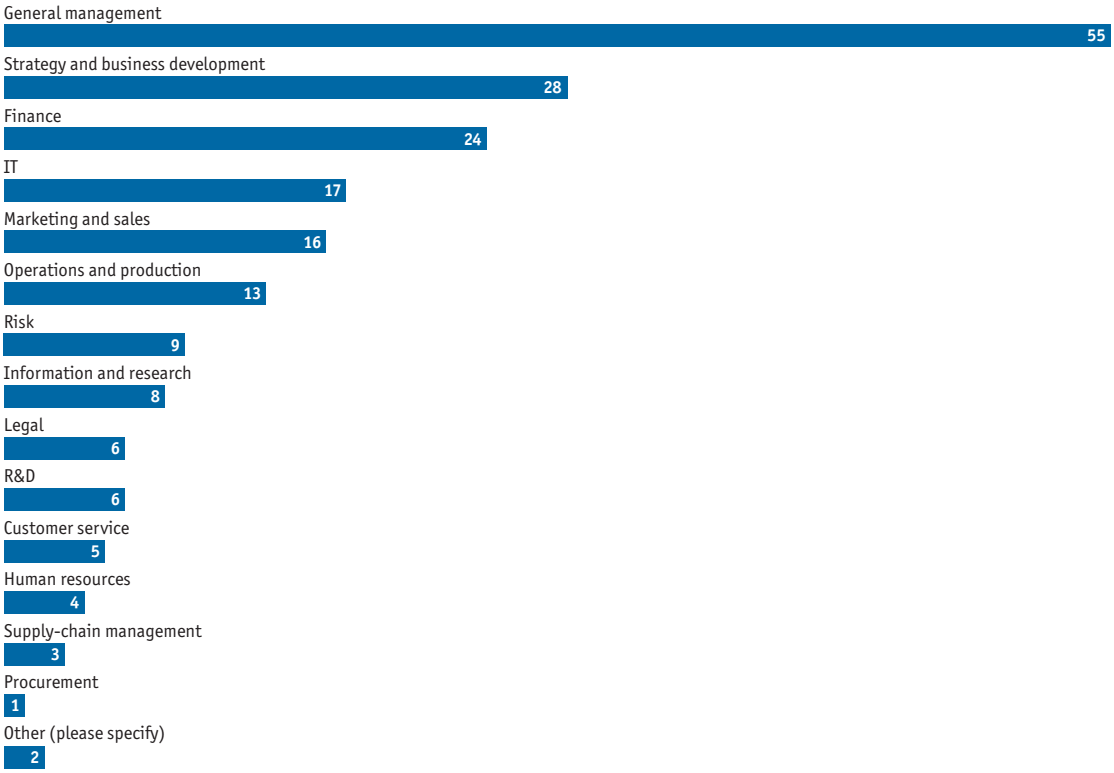


In which region are you personally located?
(% respondents)

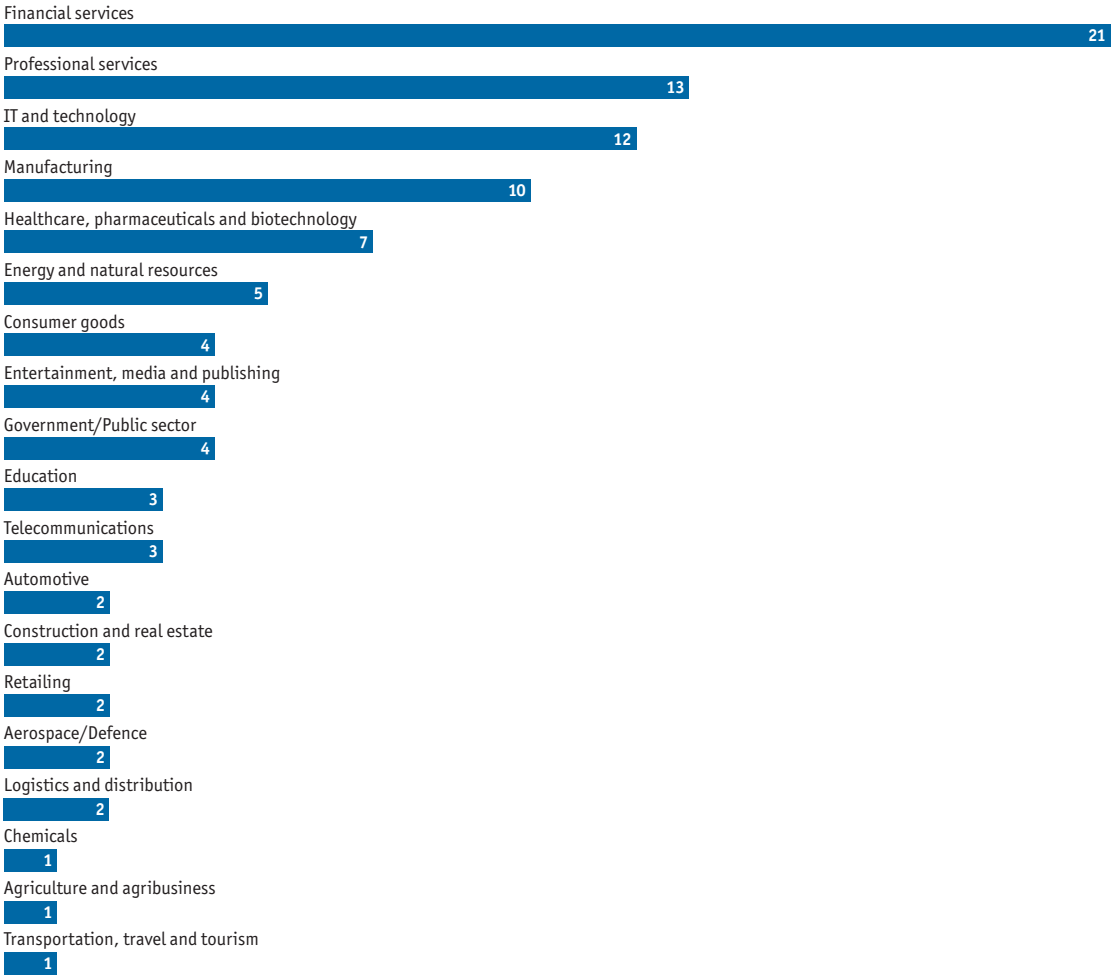
Which of the following best describes your title?
(% respondents)



What are your main functional roles? Select all that apply
(% respondents)



What is the primary industry your organisation is in?
(% respondents)



What is your organisation's annual global revenue in US dollars? Please select the most appropriate option if your company does not report revenue in US dollars.
(% respondents)

The Economist Intelligence Unit

LONDON
20 Cabot Square
London
E14 4QW
United Kingdom
Tel: (44.20) 7576 8000
Fax: (44.20) 7576 8500
E-mail: london@eiu.com

NEW YORK
750 Third Avenue
5th Floor
New York, NY 10017
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 1181/2
E-mail: newyork@eiu.com

HONG KONG
6001, Central Plaza
18 Harbour Road
Wanchai
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
E-mail: hongkong@eiu.com

GENEVA
Rue de l'Athénée 32
1206 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
E-mail: geneva@eiu.com