www.pwc.be

A matter of when, not if, a breach will occur

Information Security Breaches Survey 2016
Key takeaways

pwc

Contents

Survey carried out by:

infosecurity BELGIUM

Infosecurity.be takes place on 15 and 16 June 2016 at Brussels Expo, at the same time as the trade show Storage Expo (data storage and management) and the Tooling Event. Infosecurity.be offers ICT professionals an overview of the latest security technologies, products and services. More than 110 exhibitors guarantee a wide exhibition programme. The keynote sessions, comprehensive seminar programme and other activities at the show also offer a great deal of inspiration for all your security issues.

More information on www.infosecurity.be.

pwc

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

Our security practice, spanning across our global network, has more than 30 years of experience, with over 90 information security professionals in Belgium and 3,500 globally. Our integrated approach recognises the multifaceted nature of information security and draws on specialists in process improvement, value management, change management, human resources, forensics and risk. PwC has gained an international reputation for its technical expertise and strong security skills in strategy, design, implementation and assessment services.

More information on www.pwc.be.

Introduction

For many, 2015 will be remembered as the year the extramarital affair-enabling website Ashley Madison was breached and 37 million client records were released online. For others, it was the year the U.S. Office of Personnel Management was compromised and up to 25 million federal workers' records were stolen, including their social security numbers and 5.6 million sets of biometric fingerprints. That year also saw well-known security firm Kaspersky hacked by a suspected state actor and the Italian surveillance company Hacking Team, which specialises in the development and sale of spy tools to governments, being breached itself and its secret list of customers published online along with a large number of corporate email messages.

Belgium was not spared. The Belgian daily *Le Soir* was subjected to a sustained Distributed Denial of Service attack which almost prevented the newspaper from going to press. Similar attacks were also carried out against lalibre.be and dh.be. A Tunisian Islamist militant group claimed to have carried out the attacks in response to Belgium's involvement in the US-led bombing campaign in Iraq and Syria against the so-called Islamic State. The hacktivist group Anonymous subsequently announced that it had uncovered the identity of the perpetrators and transmitted the information to law enforcement. Six months later however, Anonymous claimed attacks on various Walloon and Brussels regional government websites in protest against perceived threats to press freedom.

The list of victims is long and a number of the companies affected have since ceased operations. The magnitude of stolen or leaked data is sometimes jaw-dropping. In many cases, careless mistakes were made which enabled attackers to gain an initial foothold in the organisation's network, from which further attacks were launched. In others, the breach required attackers to stealthily leverage multiple, privately-held vulnerabilities in key systems to compromise their targets. Proactive detection was usually sizeable and often relied on advanced threat intelligence capabilities.

Once a breach has been contained, organisations are faced with an immense clean-up operation, spanning infrastructure and systems, potential financial fines, legal proceedings and fees. A long journey of brand rehabilitation awaits those that manage to survive. Many do not. The lesson fortunately being learned is that it's not a question of whether they'll be hacked, but when. Their challenge is to ensure their arsenal is adequately prepared to successfully deal with a breach, and emerge from the experience battle-hardened.

Executive Summary

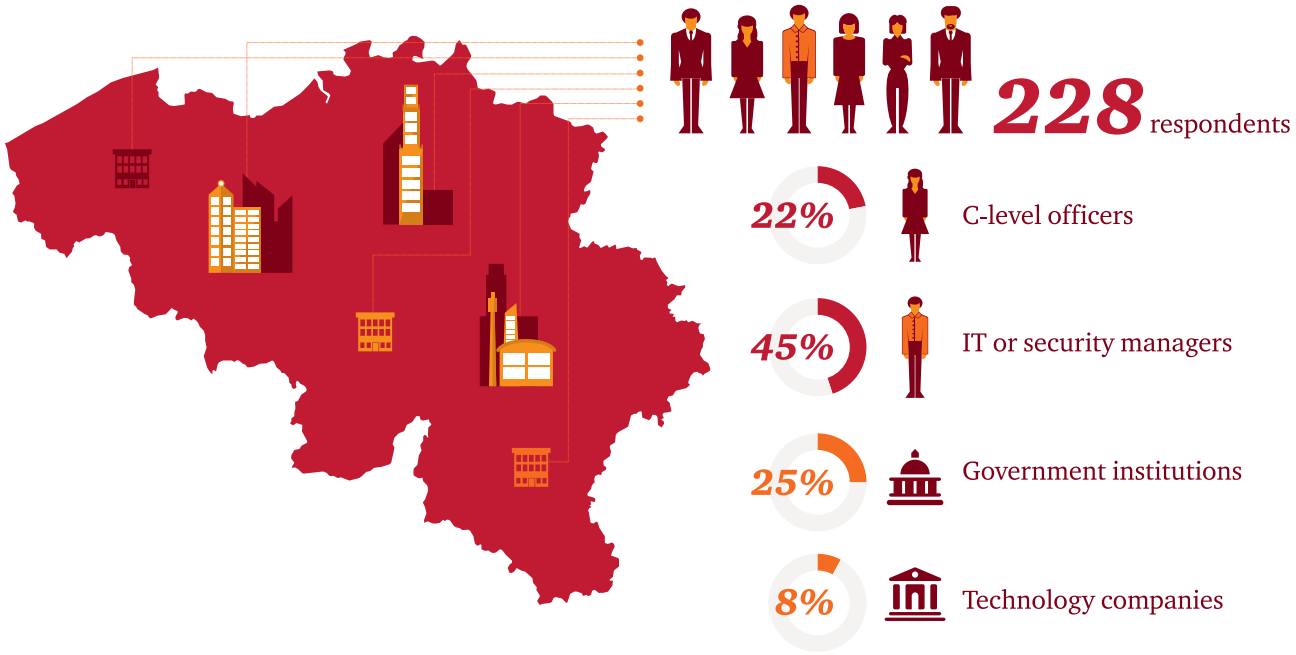
The results of the 2016 Information Security Breaches Survey suggest that while no dramatic changes have occurred in the state of information security in Belgium, organisations nevertheless continue to reduce their risk of exposure to cybersecurity threats. Information security budgets are growing, viruses and malware continue to be seen as the worst kind of breach and overall the number of organisations reporting having had a serious breach rose (from 9% to 17%). The reported financial, reputational and business impact of breaches remains low with clean-up representing the main cost.

Organisations are increasingly addressing the risks of breaches and improving their ability to deal with them, compared with previous years. A growing number have a formal incident response process in place, including a CERT, more contingency plans are being deployed and, importantly, more respondents report their effectiveness following a breach. The threat from mobile is also more widely managed and data ownership throughout enterprises is reportedly clearer than last year.

At the same time, companies are addressing the lack of security awareness among employees; there's a noticeable shift from induction-based training to continuous education. Finally, organisations are increasingly taking measures to gain insights into the security of external providers to which they delegate an ever-growing share of important data and services.

Methodology

The 2016 Information Security Breaches Survey is a study by PwC Belgium and Infosecurity.be. The survey was conducted online from November 2015 to February 2016 with respondents representing organisations based in Belgium.



There were 228 respondents to the survey, from both large companies and SMEs, the majority of whom are active in their organisation's IT and information security domains. Twenty-two percent of survey respondents were C-level officers and 45% IT or security managers. Twenty-five percent of the organisations surveyed were government institutions. Technology companies, those in the banking sector and services companies represented eight percent each of the total.

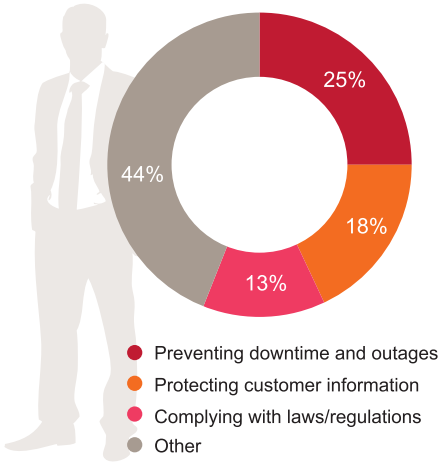
C-level officers are defined as respondents who describe their role as Chief Executive Office, Chief Technology Officer, Chief Information Officer, Chief Information Security Officer or Chief Financial Officer. Technical staff were defined as respondents who describe their role Security Administrator, Security Engineer, Security Manager or IT Manager.

To enable meaningful year-on-year comparisons, this year's survey broadly kept the same questions as in 2015, with only minor changes, to allow further insights to be gathered.

Information security spending

Drivers for information security spending remain unchanged since last year. Preventing downtime and outages is still reported to be the main driver for a quarter of respondents, followed by protecting customer information for 18%.

Drivers for information security spending



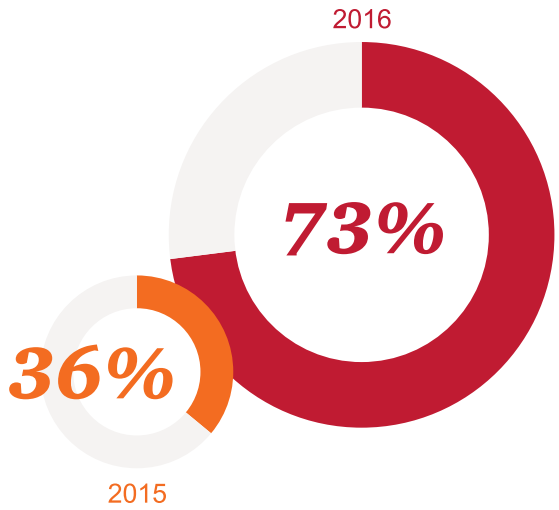
There is, however, **more alignment between the views of technical and C-level respondents about drivers for spending**. Whereas last year the top two drivers of spending differed between C-level and technical respondents, this year the top three drivers are the same for both groups (preventing downtime and outages, protecting customer information, complying with laws and regulations). The ambition to prevent downtime and outages, while a reasonable driver of information security spending in itself, may reflect an increased move towards companies offering service-based solutions. For that, availability is critical.

The 2015 Information Security Breaches Survey report highlighted upcoming changes in European data protection regulation and predicted increased attention to compliance with laws and regulations among organisations fearful of running afoul of them. This is borne out by the numbers in the 2016 results with a 71% increase over last year in respondents citing compliance with laws and regulations as a driver of information security spending. The replacement of the current ageing Data Protection Directive 95/46/ec reached another milestone when its successor, the General Data Protection Regulation (GDPR) was generally agreed upon by the European Parliament and Council in December 2015. The GDPR extends the Directive with new obligations around breach notification, data anonymization and required appointments of data protection officers. The EU aims to formally adopt the Directive in early 2016 with a two-year transition period before it comes into force in the spring of 2018. Non-compliance may lead to hefty fines.

Interestingly, while preventing reputational damage to the organisation gets the same amount of concern as last year (roughly 8-10%), it's accompanied by double last-year's percentage of organisations who state that breaches were only known about internally. **In 2015, 36% of respondents indicated a breach was only known about internally, this year that number rises to 73%.**

Of note is the low percentage of respondents for whom protecting intellectual property is a critical driver of information security spending, both this year and last. The fact that no respondents acknowledged losses above €10,000 - notwithstanding the 25% of respondents unable to quantify the value of lost assets as a result of a breach – suggests that organisations have difficulties valuing all their assets and prioritising which to protect, and effectively communicating those priorities to all staff members vertically throughout the organisation. These are key reasons to conduct Business Impact Assessments.

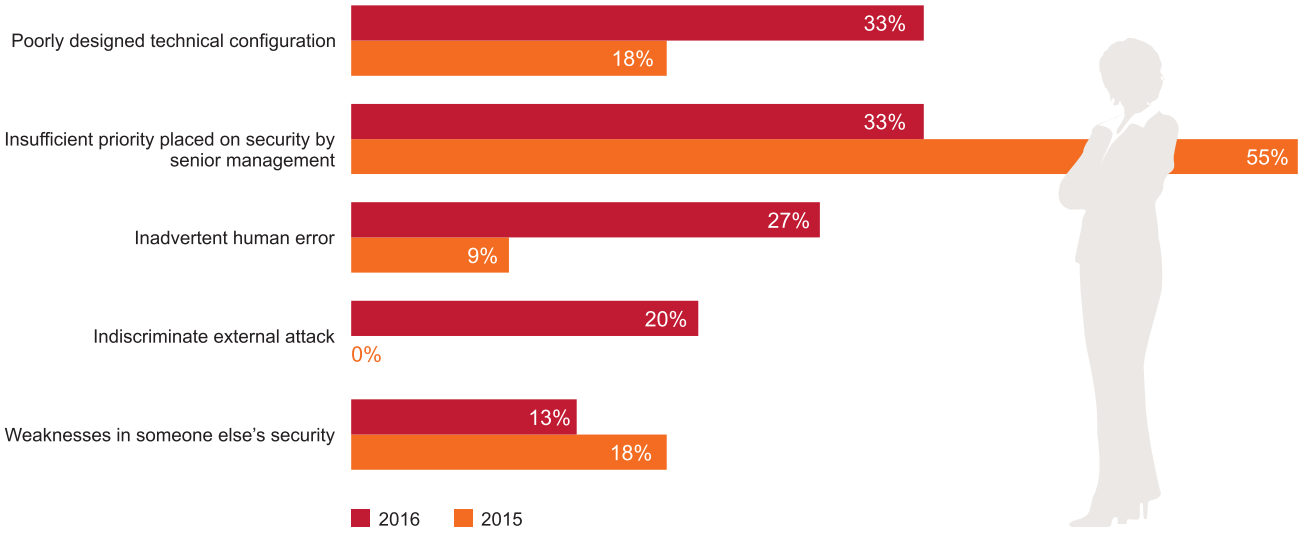
Respondents indicating a breach, only known about internally



Breaches

The number of respondents reporting having experienced a serious breach this year grew to 15% from nine percent last year, while the number of respondents claiming not to have experienced a breach remained constant at around three quarters of respondents. This increase is due to fewer respondents not being able to answer the question (8% in 2016 versus 17% in 2015). While the lack of increase in serious breaches reported may at first glance appear comforting, it should be seen in the light of other reports, such as FireEye's claim that malware or other breach indications are discovered during approximately 70% of the Proof of Concept exercises they conduct at organisations.

Cause of breach



Causes

Globally, breaches are still mainly attributed to management putting insufficient priority on security, according to 33% of survey participants, though not a single C-level respondent agrees, echoing the stark contrast reported last year between C-level and technical workers. This year saw a shift in attribution however, half of C-level respondents blame their breach on indiscriminate external attacks and another half on poorly designed technical configurations, while a quarter blame a failure to keep technical configurations up to date. The leading cause of breaches last year (67%) according to C-level respondents was weaknesses in someone else's security. This year, not one C-level respondent reports it as a cause. The shift towards blaming indiscriminate external attacks, the *modus operandi* for most cybercriminal campaigns, may be attributed to greater awareness and visibility of campaigns, but doesn't shed light on the vulnerability leading to the breach.

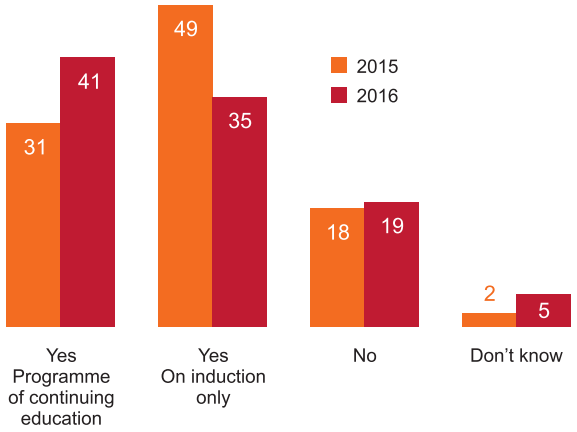
A closer look at breaches described by respondents who report insufficient priority placed on information security by senior management offers various examples; infection by viruses, attacks on websites, malicious misconfiguration of systems or legal and regulatory violations.

Results show an interesting trend when looking at the role human error plays in security breaches. Half of technical respondents attribute the worst breach to inadvertent human error, but this was not reported by a single C-level. This implies that the true cause of a breach may often be misattributed – possibly for fear of retribution. Good due diligence requires sufficiently robust audit controls to enable correct root cause determination and make sure adequate remedial actions are taken to prevent repeated costly mistakes.

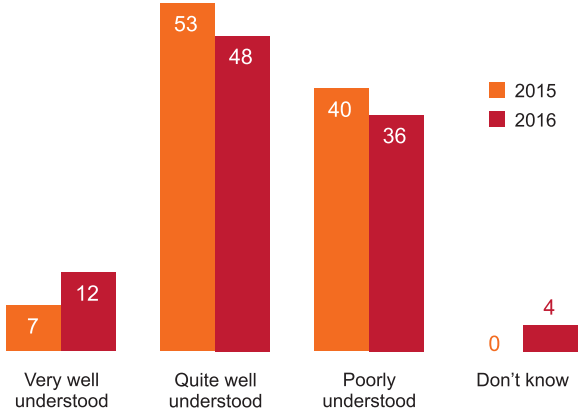
Last year's survey showed that 52% of organisations only offer security awareness training once, during induction when new hires join the firm. Continuous education programmes were limited to 31% of organisations. This coincides with a substantial percentage of respondents (47%) attributing security breaches to lack of staff awareness of security risks. This year, that number plummets to 13% and there's a corresponding rise in the reporting of continuous education programmes (41%). Unfortunately, this increase in education doesn't appear to have much effect on the number of employees perceived to understand the organisation's security policy. The seven percent of respondents who thought the security policy was very well understood last year increases to 12% this year, whereas those who thought it quite well understood decreases from 53% to 48%.

There's no noticeable difference from last year in respondents reporting breaches related to social networks (5% in 2016 versus 1% in 2015) or those who don't know whether they've been the victim of a social-network-related breach (19% in 2016 versus 26% in 2015). Perhaps surprisingly, results show a similar status quo for mobile-related security breaches. Only three percent of respondents this year report experiencing a mobile-related breach compared to five percent in 2015, and 27% don't know compared to 32% in 2015. The PwC 2016 Global Survey on Information Security reports an increase of 36% in attacks on mobile devices between 2014 and 2015. While the higher number of attacks didn't necessarily result in breaches, it's reasonable to expect (and experience confirms) that a number of attacks do result in a successful breach. It's therefore likely that some mobile-related breaches go undetected. Regardless of the number of reported breaches, there's a noticeable proactive move towards managing the security of mobile devices, as shown by the continued year-on-year growth in organisations developing a security strategy for mobile (29% in 2014, 44% in 2015, 55% in 2016). This in turn has doubtless at least partially driven the corresponding increase in the reported adoption of Mobile Device Management (MDM) solutions (27% in 2014, 35% in 2015 and 48% in 2016).

Do you provide staff with any security awareness training?



How well do you think your staff understand your security policy?



Impact

Far more money is spent responding to incidents than the worth of any data stolen. Sixty percent of respondents report no financial value of stolen data, 13% less than €10,000 and 27% simply don't know. This represents a large change over last year when 18% of respondents reported no losses and suggests that as businesses come to rely more on cloud-based services, they're moving their valuable data there, thereby reducing the value of data exposed to theft within their networks.

This observation is directly confirmed by respondents; 33% claim an incident was the worst because of the cost to investigate and fix it (no responses attribute it to the value of lost assets). Another 33% state reputational damage, but 27% claim business disruption made the incident the worst breach of the year. Last year, half of the respondents (50%) claimed cost to investigate made the breach the worst and 17% pointed towards business disruption and an equal amount to reputational damage.

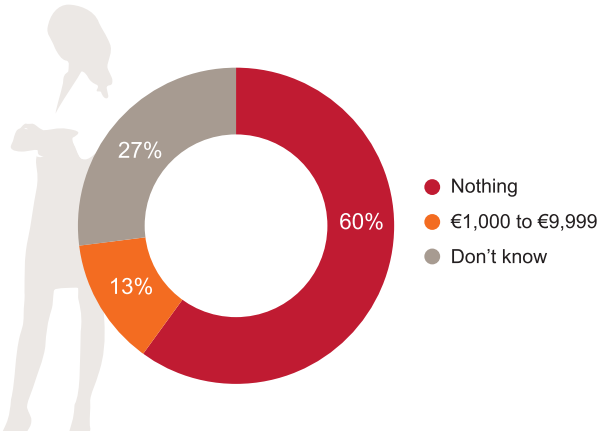
With regards restoration of business operations to normal, 40% claim it took between a day and a week. Overall, this restoration effort cost 60% of respondents between two and 10 man days, while for 20% the cost rises to between 11 and 50 man days.

The fact that no valuable data was stolen, but significant effort was required to restore operations to normal suggests that some organisations may wish to weigh the cost of maintaining their current infrastructure against transferring the responsibility for its ongoing security to a third party. Possible options for doing so include increased use of cloud-based services, where possible, using either Software as a service (SaaS) or Infrastructure as a service (IaaS) models, or indirectly via the purchase of insurance policies which include the cost of disruption to business. The latter approach is adopted by 15% of respondents, with a further 10% reporting specific cyber insurance. This is higher than last year's figure of 10% who reported having an insurance policy to cover the cost of a breach.

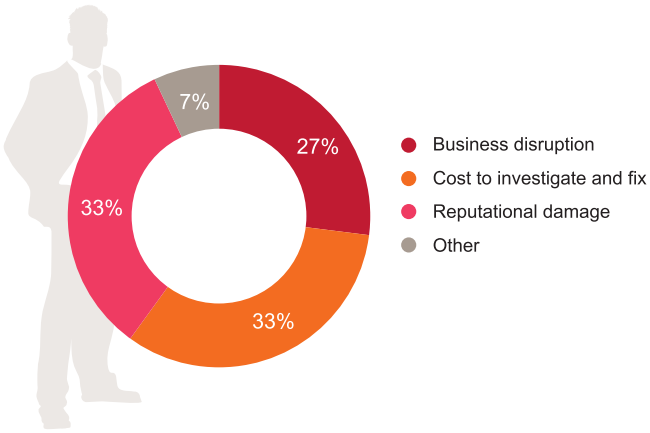
The vast majority of respondents (87%) report minor to insignificant impact on business operations during the incident, suggesting that the cost of clean-up may be reduced by, for example, adopting better business continuity management practices.

While breaches involving the theft or unauthorised disclosure of confidential data are considered to be the worst by 25% of C-level respondents, another 25% are unable to estimate the value of the lost or stolen assets. This suggests that the true cost of breaches is probably still under-reported.

What was the value of any lost or stolen assets (including intellectual property or commercially sensitive data)?

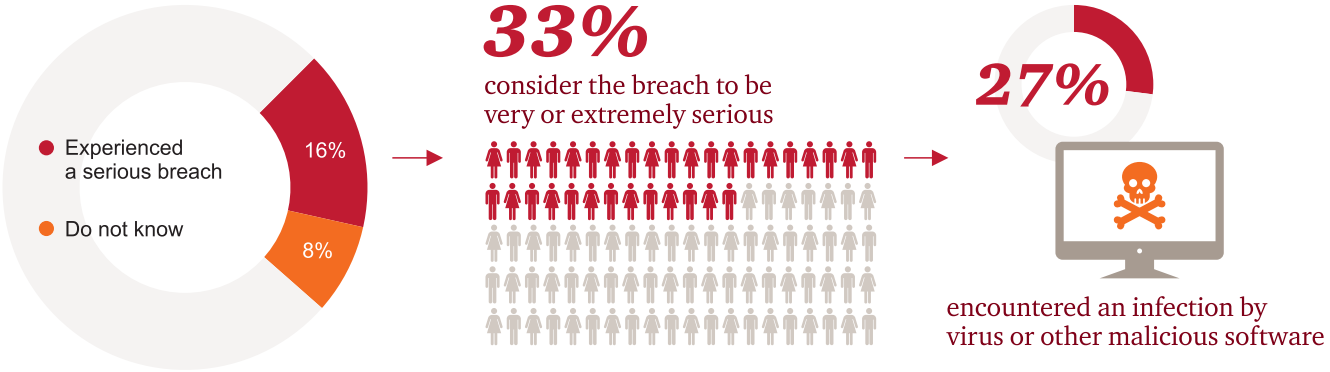


What made this incident the worst of the year?



The fact that no valuable data was stolen, but significant effort was required to restore operations to normal suggests that **some organisations may wish to weigh the cost of maintaining their current infrastructure against transferring the responsibility for its ongoing security to a third party.**

Handling



Sixteen percent of respondents experienced what they consider a serious breach in the past year (8% did not know whether they had or not). Of these, 33% consider the breach to be very or extremely serious. The worst breach for 27% of respondents was infection by virus or other malicious software. Theft or unauthorised disclosure of confidential data, fraud or theft using computer systems and attack on website or Internet gateway all averaged similar scores of around 13%. These numbers are similar to those of last year.

What type of incident was your worst breach this year?

As was the case in 2015, C-level respondents consider the most serious breaches to be virus or malware infections (chosen by 50% versus 17% of technical respondents). Theft or unauthorised disclosure of confidential data is the second worst type of breach overall. Breaches are generally thought to have been detected quickly. In 40% of cases it was within a few hours, usually through routine internal security monitoring (40% of respondents).

While 33% of respondents reported the incident to the Federal Computer Crime Unit (FCCU), over half (53%) didn't report the incident to anyone. This trend is supported by a different survey question for which 73% of respondents reported no reputational damage from a breach as it was only known about internally.

The reluctance to report cyber incidents to the authorities may be due to a concern that it'll be made public, damaging the organisation's reputational standing, or a fear of possible legal repercussions if the breached organisation is found to be lacking key security controls.

In contrast to last year, responses indicate that contingency plans are effective in dealing with security incidents. Fifty-three percent of respondents consider their contingency plans to have been effective compared to just 18% in 2015. This suggests organisations are learning and improving contingency plans to address perceived shortcomings.

External providers

Which of the following steps has your organisation taken to obtain comfort over the security at the external provider?

Although firms broadly adopt the same steps as last year to obtain comfort over an external provider's security, over 70% more respondents obtained the right to audit their provider's security. An overall increase in adopted safeguards was reported - such as requiring providers to be ISO27001 certified (28% this year vs. 23% last year) - and we note a marked drop in respondents who did nothing to increase their confidence in the security of external providers, from 14% to six percent. This increased scrutiny of partners and external providers' security may explain the 22% observed rise in firms carrying out security risk assessments covering both information security and physical security. No change from last year was reported in the number of pure security risk assessments carried out.

A lot of companies use external providers for diverse purposes; for example, almost half of survey respondents use external hosting for their company website, 29% use external providers for payroll processing, 27% for sales and/or marketing, 26% for data storage, etc. Although there's the same kind of distribution among types of application for the use of external providers as in 2015, there are more companies that don't use externally hosted solutions at all (from 10% last year to 17% this year.). This may be due to the fact that "weaknesses in someone else's security" was determined as a contributing factor for a breach by 18% of respondents to the 2015 survey.

External providers may store data or provide services that are company-critical or store highly confidential data. According to survey results, 75% of companies using external providers employ them for either business-critical service/data, confidential data or both, a slight rise from last year's figure (70%). Going into greater detail, 68% of respondents say that the data/service is important but not critical, while 22% identify the data/service as critical. With regards data, 44% have confidential data with their third-party provider, while for nine percent of companies the data is highly confidential. Calling on external providers means less work to manage internally, but it also means firms are not fully in control of the security process protecting their data.

Results indicate that most companies are taking measures to make sure that third-party providers offer good levels of security. Half (50%) make sure that their contract includes provisions for security, 43% retain the right to audit the provider's security, 28% insist that the provider is certified ISO27000 and 28% obtained a service auditor's report.

Looking more closely at the data, it appears that out of these companies, 10% experienced a security or data breach related to an external provider that compromised critical and highly confidential data.

Breach prevention

The various widely publicised incidents of advanced persistent threat actors successfully compromising targets regarded as both sensitive and secure - including components of critical national infrastructure - has served to highlight the difficulty of protecting an increasingly blurred and vanishing perimeter. As advanced attackers benefit from ever-more porous network boundaries – facilitated by the continuous advent of mobile, bring your own device (BYOD), the Internet of things (IoT), deeper integration with partner networks and services, etc. — and ever-larger data sets to target, organisations are coming to realise the importance of distributed, shared threat intelligence services in identifying indicators of suspicious activity which might otherwise pass unnoticed. Survey results show a 10% increase in investment in threat intelligence over the past year with 40% of this year's respondents indicating they make such investments. The greater visibility into advanced threats may be a contributing factor to the observed small rise in the number of respondents indicating they're quite or very confident that they can detect the latest generation of attacks designed to evade standard protection tools. Although there's a lack of change since last year in respondents' confidence in their ability to access sufficiently skilled people to manage security risks.

In addition to investments in improved detection and defence capabilities, organisations are also increasingly cognisant of the fact that the risk of a breach cannot be sufficiently mitigated by technological means alone. This explains why cybersecurity insurance is one of the fastest-growing sectors in the insurance market. While globally, cybersecurity insurance is seeing increased adoption – 59% of PwC's Global State of Information Security® Survey 2016 respondents have purchased a cyber insurance policy -, adoption rates in Belgium are lower, but growing. Whereas only four percent of respondents in 2015 reported having a cyber insurance policy and 17% didn't know it even existed, the number of insured respondents this year is 10%, with the same number reportedly unaware of its existence.

While security is often not the primary driver of adoption of cloud-based infrastructure and services, organisations moving data to the cloud, especially non ICT-focused ones, frequently benefit from improved security as a result of the move. However, these security benefits come with a cautionary caveat about the importance of good requirements management during the contract awarding process.

Only 4% of respondents in 2015 reported having a cyber insurance policy. For 2016 the number is 10%.

Future of breaches

The past few years have seen a shift from the generally accepted paradigm of strengthening organisational perimeters to prevent attacks from occurring to progressive acknowledgement and acceptance that a breach will inevitability occur. As a result, organisations are adopting more risk-based frameworks to both drive due diligence for reasonably controlling risks and to update their information security spending. Repeated breaches of organisations, including those previously considered secure, and ever-more widely publicised incidents of advanced persistent threat actors have gradually contributed to the realisation that no organisation is safe, and that rather than exclusively planning to prevent a breach, strides must be taken towards early detection and containment. Almost 60% of respondents are sure there'll be an increase in cybersecurity breaches next year (an increase over last year's numbers) and less than a quarter are confident they'll be able to detect the latest generation of attacks.

This shift has resulted in reduced stigma associated with suffering a breach. Increased legislation requiring the timely disclosure of breaches at the risk of hefty fines, combined with more prominent national and international cybersecurity-focused law enforcement bodies such as Europol and the FCCU, mean organisations are more and more likely to disclose a breach.

How an organisation handles a breach is increasingly seen as a key indication of its commitment to security. To this end, organisations are enlarging their information security spending. Almost half of all respondents expect to spend more this year than before. The realisation that a breach cannot be fully prevented leads to a different pattern of spending. Rather than simply adding more technical defences to their arsenal, organisations are increasingly managing the cybersecurity risk. The greater focus on early detection is supported by a rise in respondents adopting threat intelligence solutions, from 29% in 2015 to 41% in 2016. The growing number of companies requiring some form of reassurance in the practices adopted by their business partners indicates that security is becoming a criterion in partner and supply chain selection. Legal requirements and the reputational impact of perceived corporate good governance continue to act as further drivers of the alignment of cybersecurity risk with corporate risk registers, and make information security increasingly business risk-driven rather than technical.

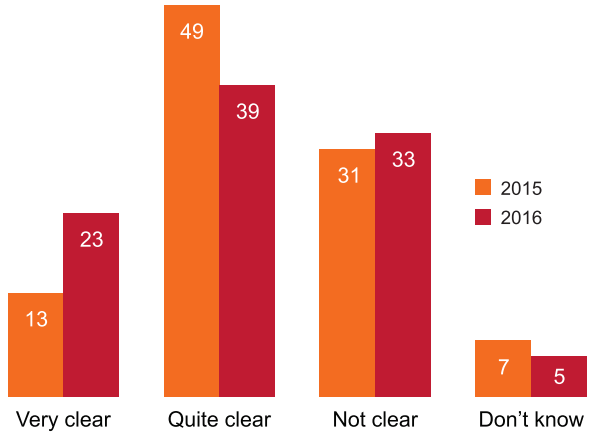
Almost 60% of respondents are sure there'll be an increase in cybersecurity breaches next year

Trends

	2014	2015	2016
Increase in mobile security policies developed	32%	47%	50%
Increase in security strategies for mobile devices	29%	44%	53%
Increased use of mobile device management platforms	27%	35%	46%
Increased enforcement of the right to audit partners	13%	23%	43%
Increased requirement for compliance with ISO 27001	13%	22%	28%
Increased investment in cyber threat intelligence	28%	29%	41%

More collection of data: Fewer respondents answered "I don't know"	2015	2016
How much money did you have to spend responding to the incident?	45%	20%
What was the value of any lost or stolen assets (including intellectual property or commercially sensitive data)?	72%	27%
How much did the incident damage your organisation's reputation?	18%	0%
Has your organisation had what your organisation considered a serious breach in the last year?	17%	8%
How long was it between the breach occurring and it being identified as a breach?	18%	7%
Do you have an insurance in any form that covers damages caused by cyber breaches?	38%	28%

How clear is it who owns critical data within your organisation and takes responsibility for ensuring the data is protected?



The coming years

Cyber threats are continually evolving, meaning cyberattacks will become more complex and more frequent; less than five percent of respondents think there'll be fewer security incidents next year (3%) and more than half think there'll be more (59%).

This foresees two major consequences, which survey results support; higher investment in IT security and reduced trust in companies.

Fifty-six percent of companies plan to spend more on IT security next year, of which 84% already raised their IT security budget last year. Only three percent plan to spend less next year. Although, as these respondents are all technicians, it's possible that they're simply not aware of budgetary spend. Compared to last year's results, there's no significant difference in respondents' vision for the future, but there's a slight increase in the number of respondents having increased their IT budget.

Companies are also anxious about the future. Just 37% are confident (very confident or quite confident) that they'll be able to access enough skilled people to manage security risks over the next year. This is exactly the same as last year, showing that corporate confidence in the evolution of Internet security hasn't changed.

Conclusions

Comparing this year's survey results with previous editions, there are a number of notable developments.

In 2015, 40% of respondents claimed that the breach their organisation experienced wasn't disclosed, that number leaps to 73% this year. This may be because the reputational damage caused by disclosing such a breach can be huge, so firms may try to avoid publicising the event as much as possible.

Corporate awareness has grown regarding the fact that traditional means of protection against cyber threats is becoming less effective and that a cyber breach is increasingly inevitable.

In 2015, 40% of respondents reported having a contingency plan, this number rises to 66% in 2016, indicating that organisations are increasingly asking when they'll be a victim of cybercrime rather than if they'll be. They're also preparing their actions for when a breach has occurred. The key difference with regards contingency plans is mostly their effectiveness. In 2015, 80% of C-level respondents considered such plans effective while not a single technician agreed. This year, there are no differences between C-level respondents and technicians, 50% of both consider plans to be effective.

This trend is further supported by the way cyber breaches are detected. In 2015, 29% of breaches were detected by routine internal monitoring; in 2016, this rises to 40%, showing companies' tendency to strengthen internal monitoring.

Companies also tend to invest in other non-traditional protection tools; the number of firms investing in cyber threat intelligence rose from 29% to 41%.

In 2015, security awareness training was mainly only given to employees as part of the induction process (52% on induction and 28% continuous staff education). In the same year, lack of staff awareness was cited as the cause of a breach in 47% of cases. In 2016, we see the proportion of continuous staff education rising to 41% and training only being given on induction dropping to 35%. And this year, lack of staff awareness as the cause of a breach drops to just 13%.

Based on the results of the 2016 Information Security Breaches Survey, it's clear that ongoing efforts to manage information security as an economic decision and bring the risks associated with it in line with others listed in the organisational risk register will continue. The increased percentage of respondents experiencing serious breaches, coupled with stagnant confidence in their ability to detect advanced threats or access sufficiently skilled people to manage them over the coming years will persist in driving organisations towards adopting threat intelligence services for the early detection of breaches.

The number of organisations transferring some of the risks associated with modern information security which cannot be adequately controlled by purchasing cyber insurance policies is likely to rise. While adoption in Belgium is slower than the global trend, it's nevertheless increasing and we expect it to continue to do so as the cyber insurance market itself matures and more policies tailored to broader audiences emerge.

With the EU Council due to adopt the Commission's GDPR this spring for enforcement in 2018, organisations can be expected to continue their preparations by integrating information security more meaningfully within their governance structures. As a result, more disclosure of incidents is foreseen, especially where sufficient due diligence and due care can be shown.

How we can help

PwC can help you understand the implications of today's security landscape and guide you in adopting a forward-thinking approach by applying new concepts to the unique needs of your business, your industry and your threat environment. Let us show you how to effectively combat the security threats of today and plan for those of tomorrow.

Contacts

Ivo Meertens
Infosecurity Belgium
ivo.meertens@jaarbeurs.nl

Filip De Wolf
PwC Belgium
filip.de.wolf@be.pwc.com

Floris Ampe
PwC Belgium
floris.ampe@be.pwc.com

Marc Sel
PwC Belgium
marc.sel@be.pwc.com

Peter Versmissen
PwC Belgium
peter.versmissen@be.pwc.com

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.