Breach Confidence Index

Executive Summary

ilex International

CONTENTS

METHODOLOGY

Ilex International commissioned YouGov Plc to conduce the Breach Confidence Index survey among British IT decision makers across small, medium and large businesses between 6-12 August 2015. The survey was carried out online with a total sample size of 530 IT decision makers.

INTRODUCTION

Data breaches are more prevalent than ever today. Mega breaches, such as those experienced by Sony (47,000 records stolen), JPMorgan Chase (83 million records stolen) and eBay (145 million records stolen) have rarely been out of the news in recent years. Despite the large scale of these organisations and their investment in IT security, cyber criminals are still finding a way in and by targeting these organisations, are uncovering a wealth of personal data.

"Today we stand on the frontline of a virtual war. And though the warheads launched are invisible, cyber is far from a theoretical threat. Our adversaries, whether revanchist Russia or evil ISIL are becoming ever more adept and determined to use cyber to force their advantage. Such dangers are only likely to grow. The cost of cybersecurity breaches to the UK economy roughly tripled over just the last year. Now in the order of £20 to 30 billion per year."

- Rt Hon Michael Fallon MP, Ministry of Defence (2015 Cyber Symposium)

Despite the statistics and media coverage surrounding security breaches and the impact they have on a business from reputation to financial losses, many companies still believe it won't happen to them. Ilex International's Breach Confidence Index highlights a key issue that many companies have; over-confidence. Misplaced over-confidence is worrying and potentially very costly for British businesses.

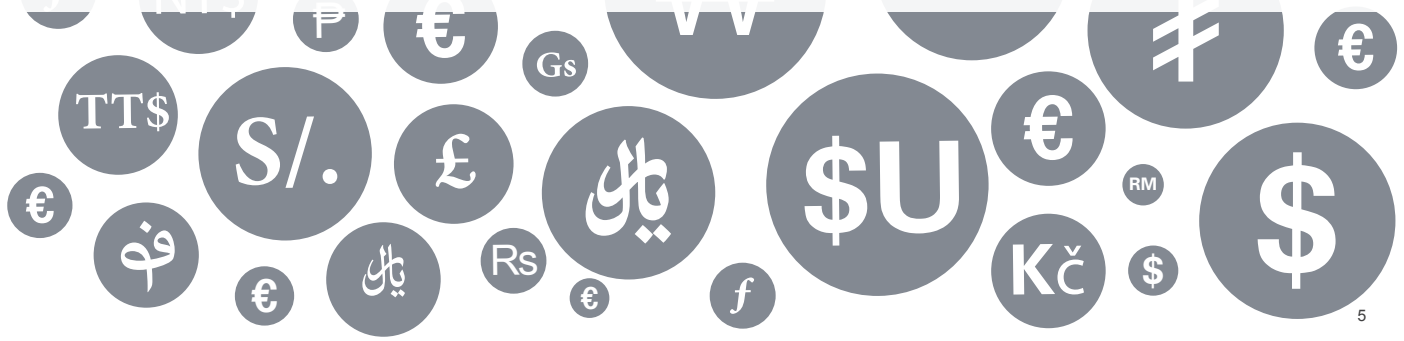
The Breach Confidence Index is a benchmark survey created to monitor the level of confidence that businesses have when it comes to security breaches. This report reveals the current level of confidence, the number of businesses owning up to an attack and the reasons they have suffered security breaches. The report aims to offer advice and best practices to help minimise the risk of a security breach.

REGULATIONS AND BREACH REPORTING

It's mandatory to report data breaches in some countries and industry sectors but there is no general rule for disclosure in Europe today. The European General Data Protection Regulation (GDPR) is currently being debated and expected to be approved by the end of 2015. By 2017, businesses across the European Union (EU) will be expected to report data breaches.

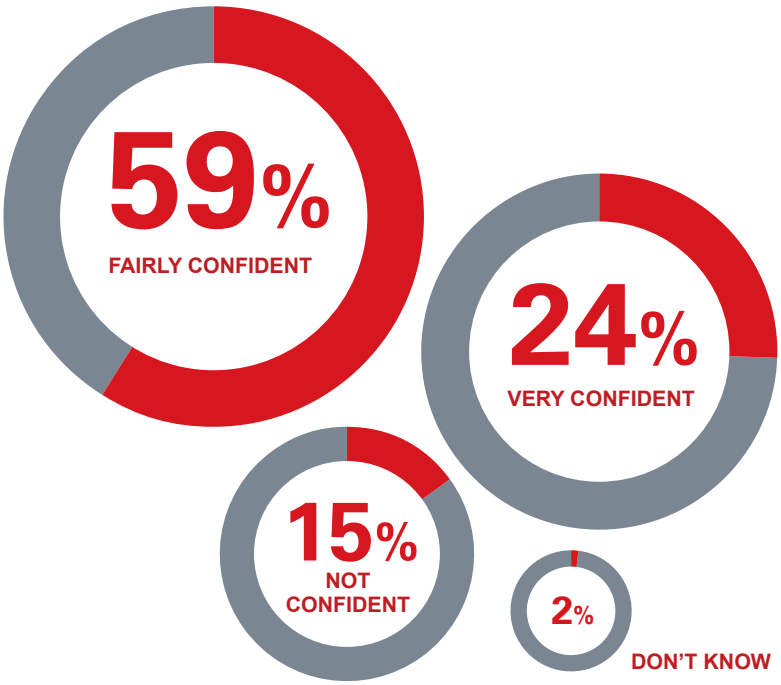
The GDPR will bring in some tough changes. Among the new rules, organisations will be required to report data breaches within 72 hours and will be liable for fines of up to five percent of their annual worldwide turnover.

Only when there is a clear, up-to-date regulation in place, where organisations are forced to report a security breach, will we know the truth about the scale of these attacks. The current hype is around the fines expected but little thought has been given to the real costs and impact that a security breach will have on businesses.



THE 2015 BREACH CONFIDENCE INDEX

The 2015 Breach Confidence Index shows high levels of confidence against a security breach. Almost a quarter (24 percent) of IT decision makers surveyed are very confident, 59 percent are fairly confident and one in six (17 percent) have no confidence or don't know if their business is protected against a data security breach.



Interestingly, when asked about weaknesses resulting in a security breach, almost half of the IT decision makers surveyed (49 percent) said that their company had not experienced a data security breach.

The results are conflicting and raise concerns following reports that the UK government has warned that 90 percent of major businesses have faced a cyberattack in the past year, with 74 percent of small businesses also victims of cybercrime*.

"With the UK being a leading economic centre and a major target for cyberattacks, the high confidence level is worrying and completely misplaced. It will be interesting to see how the index evolves when it becomes mandatory to report security breaches. Businesses are lulled into a false sense of security and we expect to see radical changes in the index when the regulation is enforced."

- Thierry Bettini, Director of International Strategy, Ilex International

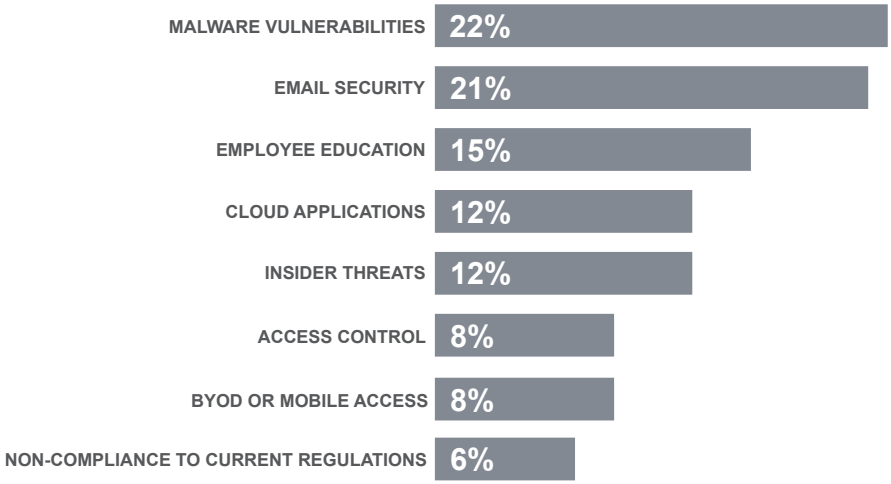
The Breach Confidence Index will monitor the changes in confidence levels among businesses as they adopt the European General Data Protection Regulation and start formally reporting on data breaches.

**Majority of UK businesses have been targeted by cyber criminals, Computer Weekly (22 September 2015)*

WEAKNESSES CONTRIBUTING TO ATTACKS

In order to minimise the risk of a data breach, it's important to understand the reasons businesses are most vulnerable today. The survey uncovers the weaknesses identified by IT decision makers that resulted in past security breaches. This report covers each issue in detail and provides further insight to help businesses close these gaps.

The most common weaknesses resulting in a data security breach, as identified by IT decision makers surveyed, include:

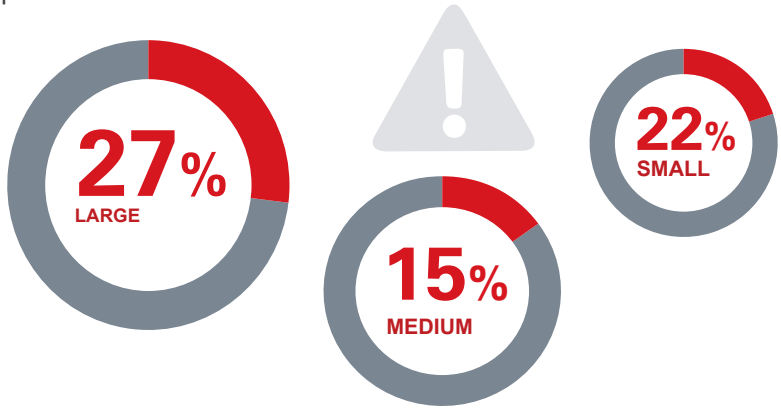


The research suggests that weaknesses relating to identity and access management considerably increase as organisations expand their workforce. Some of the most common issues highlighted by large businesses include insider threats (44 percent), employee education (42 percent), access control (26 percent) and bring your own device (BYOD) (24 percent).

MALWARE VULNERABILITIES

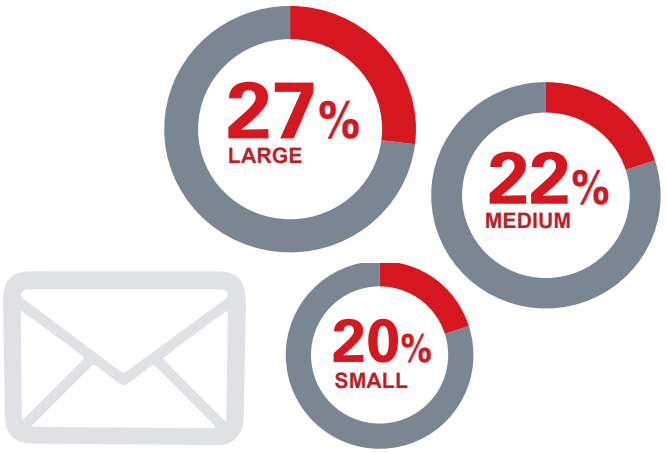
The study identifies malware vulnerabilities as a main cause of data security breaches. Twenty-two percent of respondents identified malware vulnerabilities as a reason for suffering a security breach. Both respondents from small and large organisations identified this as a key weakness, with 22 percent and 27 percent consecutively, compared to 15 percent of medium size organisations.

Malware exploits weaknesses in software code and until a patch is provided to fix these problems, organisations are vulnerable. Once it has been downloaded, malware can steal data and render a machine virtually redundant until it has been removed. In order to prevent such an attack, it is crucial for companies to install antivirus software, which as well as protecting against malware, can control network access and unauthorised access to applications.



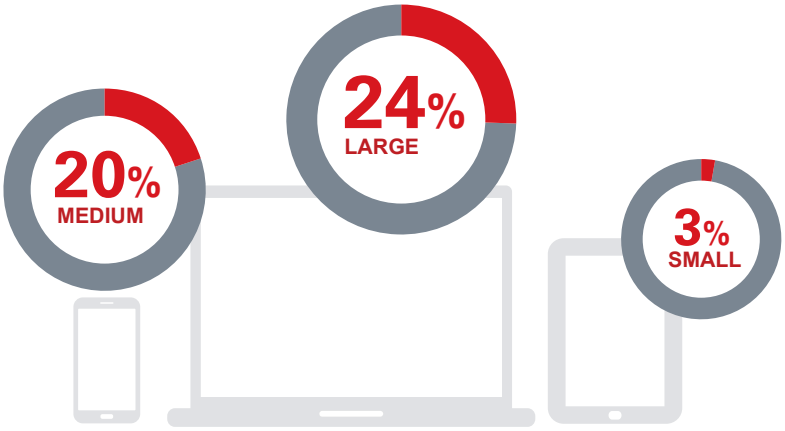
EMAIL SECURITY

Email has fast become the most commonly used method of communication for businesses. It's no surprise that email has also become a target for cyber-criminals attempting to steal sensitive company information. A gap in a company's email security strategy can enable attackers to gain unauthorised access to key accounts or infect networks by downloading malware through emails and infected files. Twenty-one percent of IT decision makers surveyed said email security was a weakness that lead to a security breach. Twenty-seven percent of large companies see email security as a weakness, 22 percent of medium and 20 percent of small companies.



BRING YOUR OWN DEVICE (BYOD)

With the growing number of new devices entering the workplace, eight percent of respondents reported that Bring Your Own Device (BYOD) was a key weakness leading to security breaches. Twenty-four percent of respondents from large organisations and 20 percent from medium sized organisations highlighted BYOD as a weakness, while just three percent of respondents from small organisations said this was an issue. Consumerisation of IT means that the changes within small businesses is minor as they are likely to use their own device from the beginning. For larger organisations, IT is playing catch up and in order to protect company data being accessed from insecure and unapproved corporate devices, more work needs to be done around security policies and education for employees using their own mobile devices.



EMPLOYEE EDUCATION

According to the research, a large number of security breaches are a result of human error – either deliberate or accidental. The lack of employee education and training on security best practices was identified by 15 percent of respondents as the cause of a security breach. Employee education is a bigger issue in larger businesses with 42 percent stating it as the reason for suffering a security breach. This dropped to 39 percent in medium size businesses and just eight percent in small businesses.

Organisations should include security awareness training as mandatory in security policies and offer regular courses to employees. Completely removing human error is impossible and therefore training should always be combined with security and monitoring technologies to limit risks.

42%

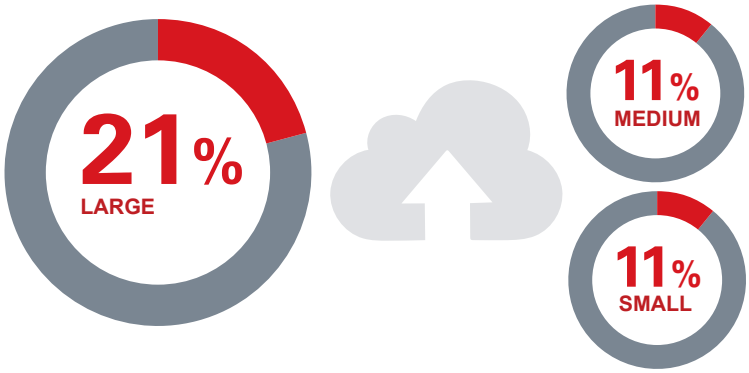
of IT decision makers from large businesses identified employee education/ lack of training on security best practices as the reason for a breach

CLOUD APPLICATIONS

As more and more businesses migrate to the cloud, targeting cloud applications has become an increasingly attractive target for cybercriminals. By moving data outside the network perimeter, businesses are losing control of their data and opening gaps which can result in security breaches.

The survey revealed that 12 percent of IT decision makers saw cloud applications as the reason for a security breach, resulting from data leaving the network perimeter. Twenty-one percent of large businesses stated that cloud applications resulted in a security breach, followed by 11 percent of medium businesses and 11 percent of small businesses.

The promise of scalability and speed makes the cloud an increasingly popular option for many organisations. However, security remains a concern.



INSIDER THREATS

Two years on from the Edward Snowden leak, insider threats remain front of mind and a major concern for many businesses. Whether or not the attack is malicious, the cost to an organisation can be high. Twelve percent highlighted insider threats as a weakness in their company. Almost half (44 percent) of IT decision makers identifying insider threats as the reason for a breach were from large businesses. Six percent were from small businesses and 15 percent from medium business.

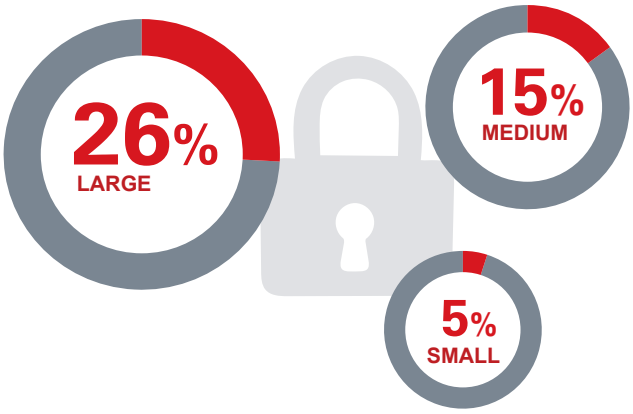
44%

of IT decision makers from large businesses identified insider threats as the reason for a breach

Insider threats are largely caused as a result of an extended enterprise – employees, ex-employees, contractors and partners - all having access to a company's network. Terminating dormant accounts, controlling access to data through strong authentication and ensuring that access to data is only granted to the right people are all basic steps businesses should put in place to keep their information out of the wrong hands.

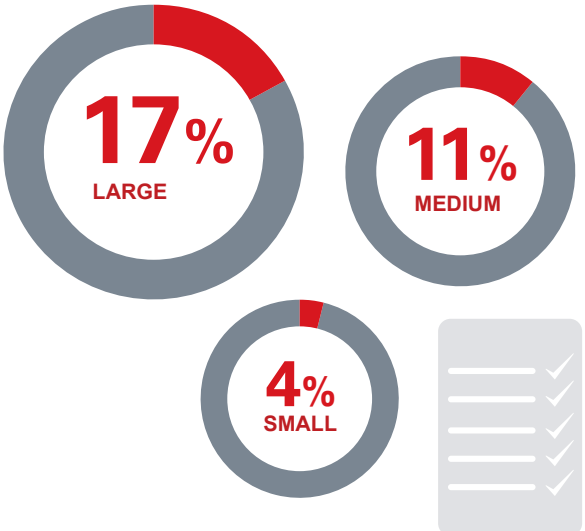
ACCESS CONTROL

Weaknesses in controlling access to sensitive data or applications means businesses are effectively leaving the door open to cybercriminals. Eight percent of respondents that had suffered a security breach blamed poor access control. The biggest proportion were from large companies (26 percent), followed by medium companies (15 percent), with only five percent of small companies highlighting access control as the reason for a breach. By putting an increased focus on access control, businesses can also minimise the security risks associated by BYOD and access to data residing in cloud applications.



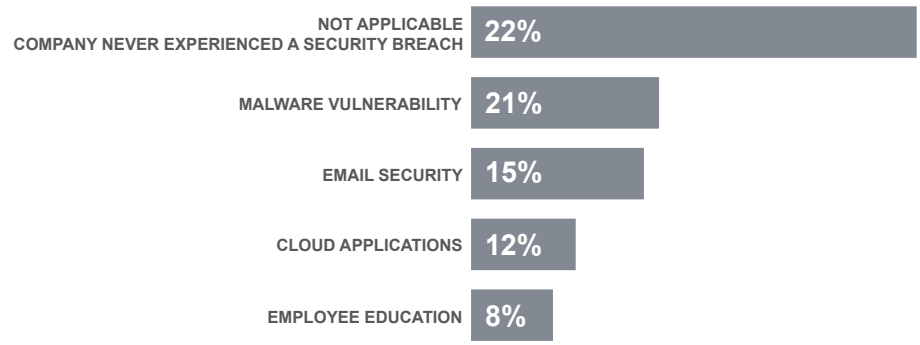
NON-COMPLIANCE TO CURRENT REGULATIONS

Despite the introduction and media hype around new regulations, such as the EU Data Protection Regulation, only six percent of respondents saw non-compliance as a reason for suffering a breach. Seventeen percent from large companies, 11 percent of medium and four percent of small businesses. Today, non-compliance to current regulations is the least common reason why IT directors believe they have suffered a security breach. Current data regulations including the UK Data Protection Act are outdated when it comes to adopting new technologies like the cloud but governance and audits require compliance. Until new up-to-date regulations come into force, it's important that businesses of all sizes review current regulations and implement best practices to minimise security risks.

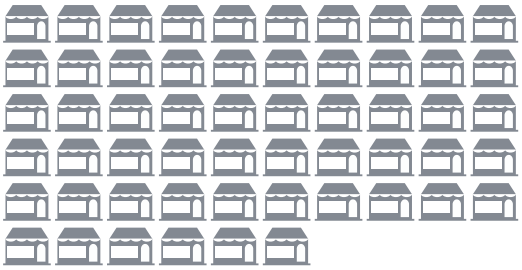


THE WEAKEST LINK

As businesses grow in size, it's clear that issues relating to identity and access management grow with them. Smaller businesses do not recognise insider threats, access control, BYOD and employee education as the most common reasons for failure in the case of an attack. In fact, over half the IT decision makers surveyed within small businesses (56 percent) stated that they had never experienced a security breach. The most common issues identified by those in small businesses that had suffered an attack included malware vulnerabilities (22 percent), email security (20 percent) and cloud applications (11 percent).



When there are only a few people in an organisation, trust levels are much higher and there are typically very few policies, processes or solutions in place to protect data. With small businesses making up such a large part of the economy and in many cases partnering with larger organisations, this mindset is dangerous. Separate research has showed that targeted attacks among smaller businesses are increasing, especially when they link into larger organisations that are the true end targets.



56%
of small businesses had never suffered a security breach

"Larger organisations with bigger and often more experienced IT security teams tend to be more aware of the current threat landscape and the sophistication of attacks today. With small and medium businesses being the main suppliers to larger businesses and making up over 99 percent of UK businesses, it's important their over-confidence isn't the downfall of security breaches in 2016. These organisations must educate themselves and their growing workforces on security best practices to minimise the risk of a security breach."

- Thierry Bettini, Director of International Strategy, Ilex International

The concern around small businesses being the weakest link is compounded when looking at expectations for 2016. Large businesses are more aligned to the current threat landscape with almost a third (30 percent) expecting a data security breach in 2016, compared to only six percent of small businesses. Overall, one in nine UK businesses expect a security breach in 2016.

BEST PRACTICES FOR BREACH PREVENTION

From education on security best practices to better access controls, there are a myriad of solutions available to protect your data. However, it's near impossible to be completely protected. With the evolving nature and sophisticated methods used in cyberattacks, combined with new technologies like the cloud and mobile, there will always be new gaps opening up and increased risks faced by organisations. Security breaches will continue to happen and attackers will always find their way into an organisation if they try hard enough – if not today, tomorrow.

The key is to focus on the data that really matters and ensure that there are tight identity and access controls in place around this data. Sensitive data should only be available on a need to know basis. Access to the data should also be closely audited to ensure only those that need to are accessing the data and investigations put in place for any anomaly.

Identity and access management is key for both large and small organisations. It represents the foundation of a secure system. Businesses can put all their time and money into securing parts of their applications or networks but if they do not know their users and control their access, it is worthless. Security should focus on preventing access to cybercriminals, not finding a solution to get them out.

Businesses should never rest on their laurels when it comes to protecting data. It's time we moved away from a false economy where so many believe that 'it will never happen to me'.

"We believe it's better to invest in digital now than pay the penalty later on. So, as the headline writers are fond of writing - we're putting our money where our mouse is - channelling more than £860 million into our National Cyber Security Programme. However, the story doesn't end here. Like the technology itself we must continually adapt."

- Rt Hon Michael Fallon MP, Ministry of Defence (2015 Cyber Symposium)

ABOUT ILEX INTERNATIONAL

Ilex International is a European Identity & Access Management (IAM) software vendor. Founded in 1989 Ilex offers a comprehensive solution including identity management (identity, rights and role management) and access management (authentication, access control, SSO, identity federation and card management). The company invests heavily in R&D, providing state of the art technology and services to a large international customer base across finance, defence, healthcare, government and retail sectors.

ILEX INTERNATIONAL

info@ilex-international.com
www.ilex-international.com/en/