Taking care of corporate security and employee privacy

Why cyber-protection is vital for both businesses and their staff

kaspersky

BRING ON
THE FUTURE

Contents

Methodology

This report is based on key findings from the Kaspersky Global Corporate IT Security Risks Survey (ITSRS) – a global survey of IT business decision makers, conducted in Q2 2019.

A total of 4,958 interviews were conducted across 23 countries. Respondents were asked about the state of IT security within their organizations, the types of threats they face and the costs they have to deal with when recovering from attacks. Regions covered include LATAM (Latin America), Europe, North America, APAC (Asia-Pacific with China), Japan, Russia and META (Middle East, Turkey and Africa).

Throughout the report, businesses are referred to as either SMBs (small & medium sized businesses with 50 to 999 employees), or enterprises (businesses with over 1,000 employees). Not all survey results are included in this report.

Contributors

Andrey Evdokimov,
Chief Information Security Officer,
Kaspersky

Alena Reva,
Head of Human Resources,
North America, HR, North America,
Kaspersky

Koen Maris,
Cybersecurity Leader,
PwC Luxembourg

Introduction

Going to work each day can be a means to an end, but it can also give us purpose, satisfaction, and even joy. There are many factors about our working lives which make getting out of bed that little bit easier – from the people we work with and the office environment, through to the buzz of the sector we work in, or the excitement of our role – not to mention pay day.

Staff are also benefiting from flexible and remote working, with more of us set to carry out tasks outside of traditional office spaces over the coming years. Employees can stay connected whenever and wherever they are needed to without having to sit right next to each other.

We don't need studies to tell us that if workers are happy, motivated and fulfilled, then they will be more productive and want to do a good job for the wider business and their colleagues. But while much focus has been put on the role of a good working environment, staff trust when working remotely and corporate culture in boosting business and employee performance, there is one area of impact on staff morale which has not been as widely addressed – a data breach. The fall-out from breaches, in terms of the individuals whose details were compromised and the financial impact on companies is often widely documented. But what about the people left cleaning up the mess? From junior members of staff through to the CISO, data breaches can have far reaching consequences for those within the company, as well as the customers affected.

The extent of a breach on employees can vary hugely – whether that's putting additional stress on their day, missing important family events, or even losing their jobs as a result. Indeed, high profile job losses in the wake of a customer data breach have made the headlines over recent years – including **Michael Johnson, the (former) CISO of Capital One and Joe Sullivan, the (former) CSO of Uber.** But it is not always just those at the top of the tree, or even just those in the IT department, who bear the brunt of the impact.

In a world driven by data, the impact on those tasked with looking after it could be far reaching and devastating, if something goes wrong. The rise in cloud technologies and SaaS have greatly benefited companies and their workforces, but individuals need to be responsible for their online actions – even when working remotely from the comfort of their own home. Although often underpinned by regulatory obligations, good data governance should be something which happens for the sake of staff morale and well-being, not just ticking boxes.

This report highlights the full impact of data protection on employees and what more businesses can be doing to ensure it does not affect staff satisfaction and company reputation. The story focuses on the human side of data breaches and the important role played by cyber-hygiene, cybersecurity practices and the right support.

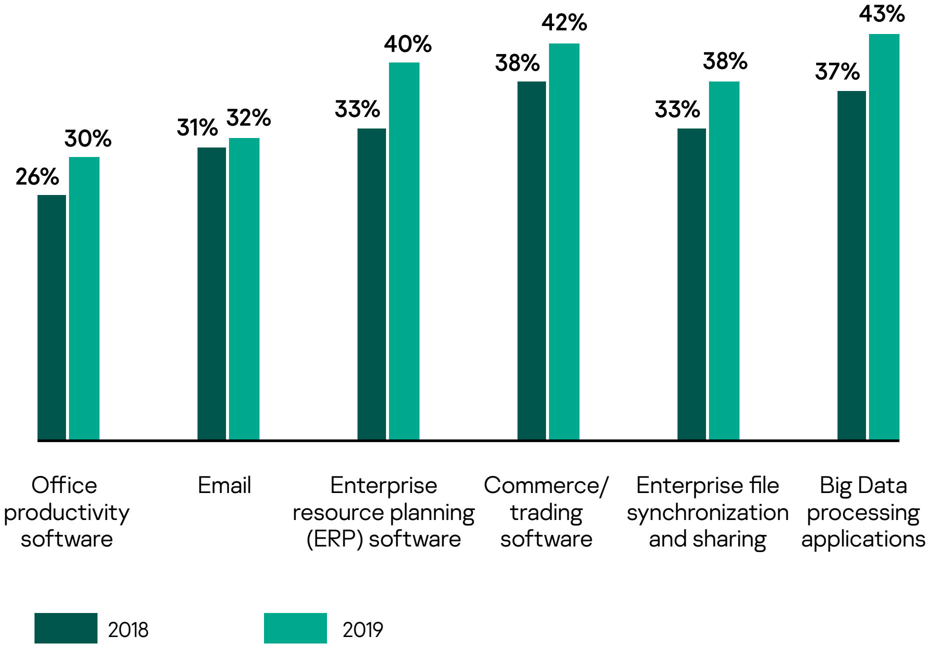
Key findings

47%	of organizations experienced data breaches in 2019
66%	of employees have been involved in the clean-up process following a breach
51%	of all data breaches have resulted in a disciplinary procedure or other consequence for employees
33%	of staff felt much more stressed at work as a result of a data breach
For 30%	of those working in large enterprises, a data breach has meant missing an important personal or family date, due to staying at work late to sort out the problem
27%	of enterprise staff are more likely to have their weekends or annual leave impacted in the event of a data breach
35%	of non-IT staff in smaller businesses faced disciplinary actions following a data breach
24%	of data involved in breaches is personal employee information

Changing workplace environments

Trying to achieve a dynamic business environment is not just a buzzword but now the reality for many businesses worldwide. Companies are using cloud services to empower employees with flexible tools so they can work from everywhere and the use of SaaS continues to grow every year. For instance, the chart below shows how there's been a rise in a variety of SaaS solutions, including office productivity software, enterprise resource planning (commonly known as ERP) software and Big Data processing applications.

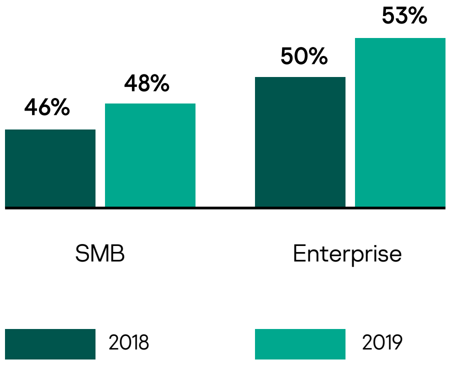
Table 1. **The growth in use of SaaS application – year-on-year split,** Kaspersky Global Corporate IT Security Risks Survey 2019



The employees themselves are also used to using different support services for work or for personal needs. If business data is drifting away from corporate environment, then organizations need stress the importance of responsible attitude towards its security. Yet as data breaches are a common occurrence in many industries, with 48% of SMBs and 53% of enterprises experiencing at least one data breach in 2019, staff must remain cautious using unauthorized cloud services or working away from the office.

Despite there only being a slight increase in breaches on the previous year (as shown in the chart below), the impact on staff has not been fully assessed. Policies and procedures provide tactical steps to follow to minimize the damage to the business, but the knock-on effect on employee well-being and their careers is often only realized in the aftermath of an incident. By which time it is too late for the individuals involved.

Table 2. **Percentage of data breaches in different business segments – year-on-year split,**
Kaspersky Global Corporate IT Security Risks Survey 2019



For example, the **Equifax data breach** affected 147 million people in the US, as well as 14 million UK citizens and 100,000 Canadian citizens. But despite the enormity of this breach and the number of lives it potentially affected, it was down to only 50 people to resolve. In the aftermath, individuals were singled out in the media and business world, which had a demoralizing effect on those involved – possibly damaging their personal reputation. The CISO David Rimmer was attacked for having a music degree, and employees working for the company received death threats on social media. Chief Executive Richard Smith, CIO David Webb and CSO Susan Mauldin all stepped down from their roles as a result of the global incident.

Although there are very few publicized examples of the after-effects of a data breach on staff, our research suggests that this level of impact is not an isolated occurrence. In fact, two-thirds (66%) of IT and IT security managers said they took part in remediation measures following a breach, which suggests that involvement of staff in any clean-up is widespread. These individuals are also pulled into the firing line when staff are penalized. In addition to involvement in responding to an incident, more than half (51%) have found themselves being disciplined or felt other consequences as a result of the breach.

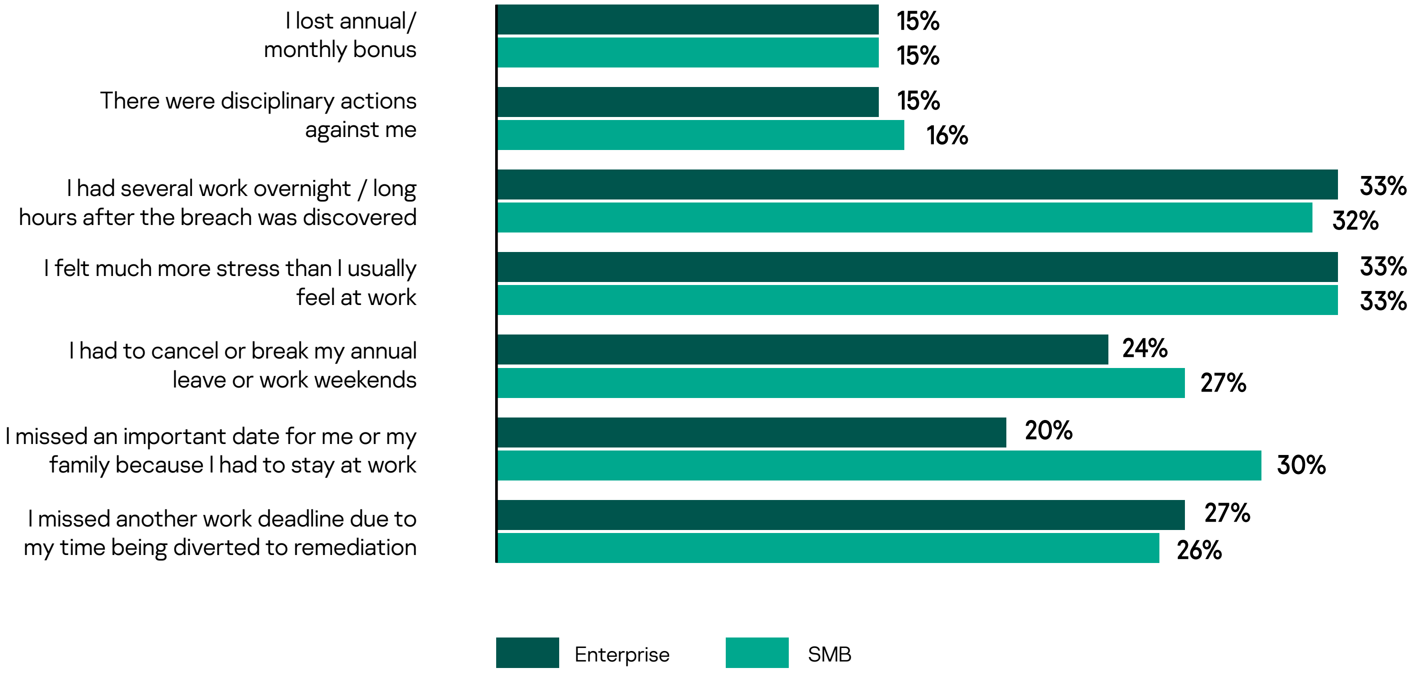
Weighing up personal consequences

Staff tasked with responding to a data breach can suffer wide ranging consequences. An incident not only affects the working day, but also life outside of the office. From family tensions, to being disciplined at work and feeling more stress, the impact of a breach can be put into three categories: social, health and work-related. In modern working environments, all employees want to be at the top of their game, but a breach could possibly affect them in all three areas.

While staff might expect disciplinary action in the event of a breach (true for 16% of those working in enterprises and 15% of SMBs), it is the more personal impacts that are more surprising and encroach on life outside of work. Nearly a third (30%) of workers in the enterprise sector have missed an important personal or family date due to working late following a data breach. It is quite easy to sympathize with somebody who may have to miss their daughter's dance contest or brother's wedding because they have had to stay late a work. More than a quarter (27%) of enterprise staff have also had to cancel annual leave or work over the weekend to resolve issues.

It's not just annual leave that suffers, workers are also missing sleep as well as vital time at home with their family. Around a third of enterprise (32%) and SMB (33%) workers said they have had to work overnight or long hours after a data breach was discovered. More than a quarter of enterprise (26%) and SMB (27%) IT decision-makers have also missed a work deadline due to time being diverted to sorting out a data breach.

Table 3. **Personal consequences of data breaches for employees in SMB and enterprise organizations,**
Kaspersky Global Corporate IT Security Risks Survey 2019



Alena Reva, Head of Human Resources, North America, at Kaspersky says that such personal consequences may affect the company's overall reputation for both external and internal audience:

"Studies have shown, and it is also common sense, that a data breach can cause substantial damage to a brand's value due to a loss in consumer trust, and it will definitely impact a company's reputation as an employer and impact its employees trust. Breaches can draw media attention, which results in unwanted public exposure, and an employee may need to answer unpleasant questions from their family members and friends.

Therefore, it is important for companies to be transparent with their people about what has happened, why it happened, what company plans to do to fix it and how employees can help. People know that anyone can make a mistake, but it's important for the company's management to stick to company values managing the aftermath, as how the company comes back from the mistake is what matters for people."

As well as impacting on personal time and deadlines, breaches can also be a source of additional stress. This is a cause for concern, with IT staff already feeling significant stress and burnout, without adding a data breach into the mix. In the UK alone, **42% of workers in the IT industry suffer from ongoing worry and feel exhausted due to long hours**. **86% of workers worldwide also suffer from work-related stress**. In fact, a third (33%) of IT decision-makers in both enterprises and SMBs felt more stress than they usually would, due to a data breach.

Different departments, similar results

While it's expected that IT staff will be impacted by data breaches, as they work closely with cybersecurity teams, our research found that no one is immune from the effects. Even those who do not work in the IT department can feel the consequences – from financial loses and redundancies to even criminal investigations.

In previous research, we found that the average cost of a data breach could reach **$141 million for enterprises and $108,000 for SMBs.** With so much at stake for the business, it's no surprise that staff outside of the IT department could find their resources and salary affected as a result. In fact, over a third (36%) of non-IT staff lost their bonus due to a data breach. Even a fifth of senior non-IT executives in enterprises (21%) and SMBs (19%) lost out too – showing how breaches affect people at every level.

Table 4. **Consequences of data breaches for employees in small and medium businesses,** Kaspersky Global Corporate IT Security Risks Survey 2019

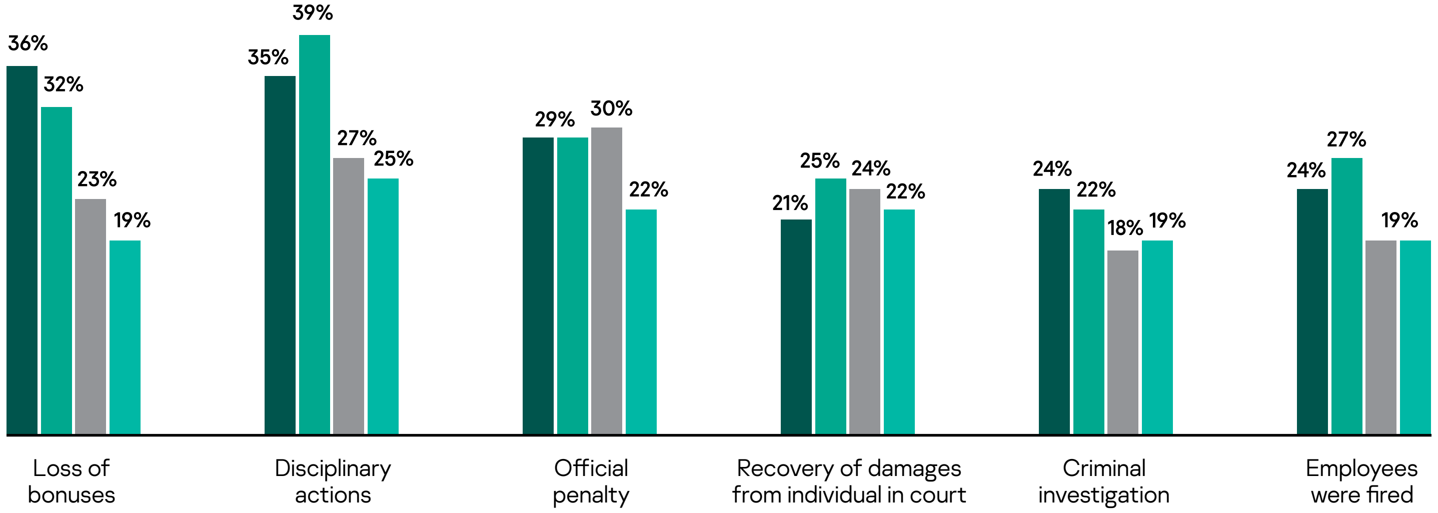
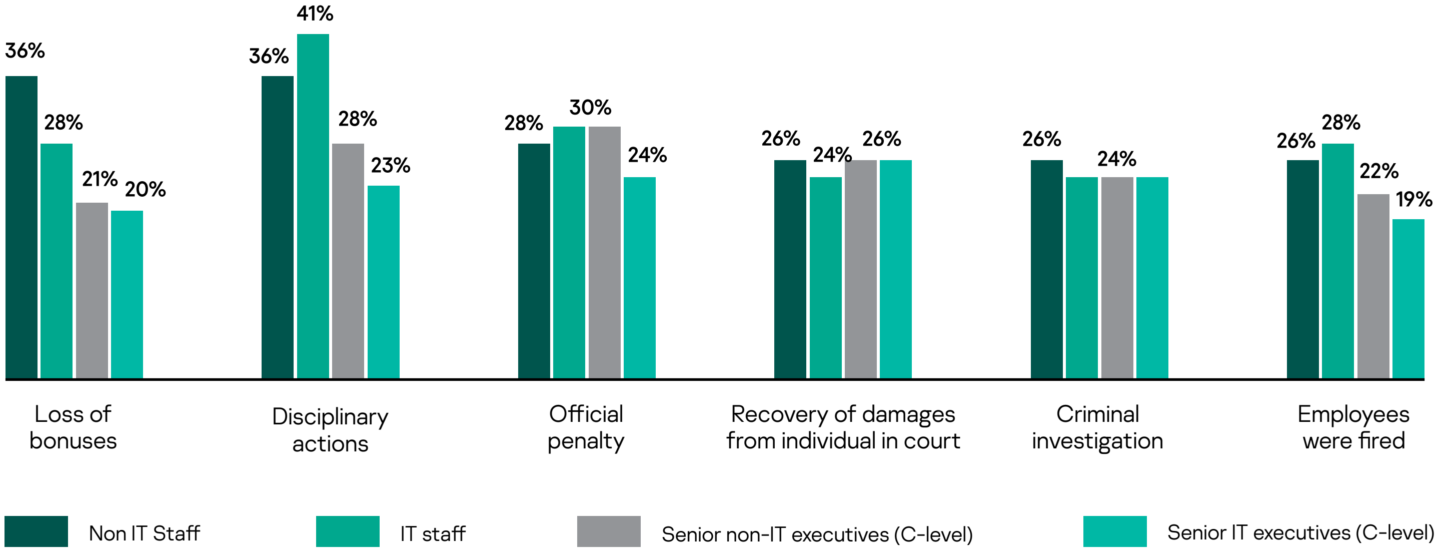


Table 5. **Consequences of data breaches for employees in enterprises,** Kaspersky Global Corporate IT Security Risks Survey 2019



Employees don't necessarily need to be responsible for cybersecurity to face the full impact of an attack. More than a third (35%) of non-IT staff and over a quarter (27%) of senior non-IT executives in SMBs faced disciplinary actions following a data breach. Around the same number (26% in enterprises and 24% in SMBs) even lost their jobs as a result.

"Unpleasant consequences of incidents can sometimes be a result of ineffective management and business processes, unwillingness to make improvements and ill-prepared staff, including IT and non-IT teams. A security incident can literally happen to any company today, so it is vital for businesses to understand what has caused it and the consequences afterwards and how to manage them to survive when processes are broken and data is unavailable."

"However sometimes businesses don't have clear picture of the incident, making the wrong inferences or taking incorrect actions not only in terms of cybersecurity, but also in terms of decision making, changing of business processes and taking organizational measures. Then the consequences may not be so severe or happen as often because of incidents but because of ineffective top management decisions. As a result, instead of improving the cybersecurity posture, employee awareness and instilling a sense of responsibility for their digital actions, and overall lesson learning organizations may prefer just to punish the guilty. I know an example of a bank where IT and IT security managers and staff are always fired because of incidents — in order to 'motivate others' to not let a breach happen. The investigation of one such incident revealed that besides dismissals, no action was taken to improve the IT system itself. This then caused new cybersecurity incidents and a new round of punishments. As a result, the bank lost many clients and its strong position among its competitors," tells Andrey Evdokimov, Chief Information Security Officer at Kaspersky.

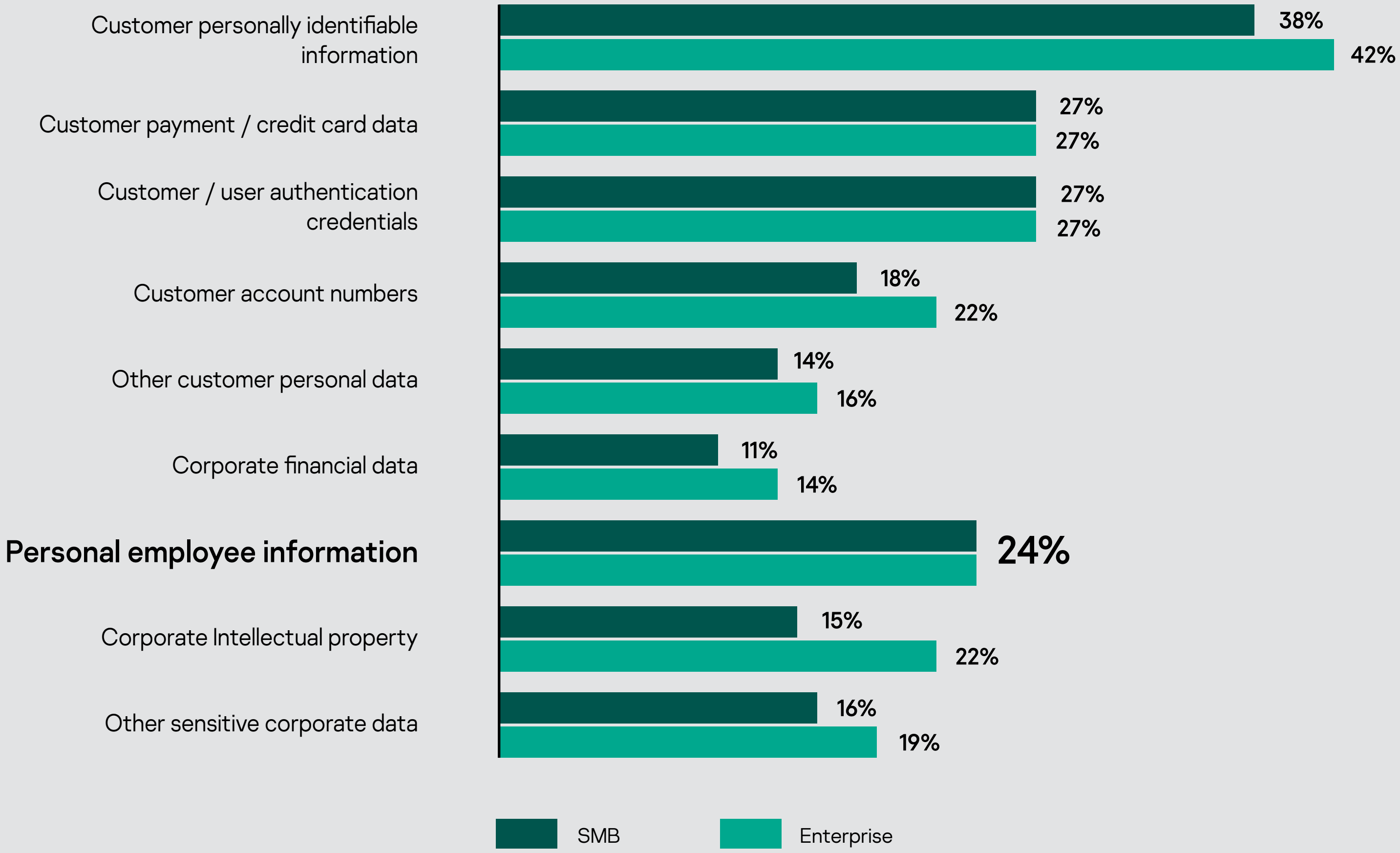
When a data breach happens, it is often heads of IT and cybersecurity who are judged and lose their job publicly. But there are some doubts that such practice is the best in this case.

"While the desire to fire a CISO facing an incident is understandable, as it's a symbolic public relations win, it's not always the smartest decision for the organization involved. It is essential to realize that CISO is an incredibly difficult position, and they are responsible for performing in something they can never provide 100% assurance on, like securing the entire enterprise. One missed vulnerability, one accidental "insecure" process, or one insider is all it takes. When it comes to replacing a CISO, time and resources spent on recruiting can be arduous and finding the right person can take a while. This time should instead be spent on lessons learned, creating, and developing processes which an existing security team would be in a better position to advise, given the knowledge they have regarding the vulnerabilities of the organization," adds Alena Reva.

Keeping staff data protected

Employees' personal information is a valuable resource for cybercriminals. With the stakes already high to keep customer data secure, companies also need to take the same steps to protect their employees' details. In 2019, thieves **stole personal banking information for tens of thousands of Facebook staff.** While this was done by taking physical hard drives, a data breach could create a similar result. Indeed, a quarter (24%) of the workers we spoke to have felt these effects, and had their own personal information compromised in a data breach. By comparison, only 14% of enterprises and 11% of SMBs have lost corporate financial data – highlighting the priority often put on protecting business over employee data.

Table 6. **Types of data involved in data breaches – SMB and enterprise split,** Kaspersky Global Corporate IT Security Risks Survey 2019



The rise in smarter technology has also led to a rise in data collection. Companies want to learn more about their customers, but this is putting pressure on employees. **Koen Maris, Cybersecurity Leader at PwC Luxembourg**, believes that time has come to understand that pressure and put process in place to protect staff, as well as data:

You are a data cluster!

People active in cyber have all digital substitute, call it your digital twin or your digital shadow. The name reveals the subject, and subject is you. Corporations suffer from an unsatisfiable hunger for data, the more the better because today they can. We come a long way, in the early day's storage capacity was worth gold. Which lead to a phenomenon where companies carefully selected what to collect and what not. Later storage capacity significantly became cheaper, but the compute power available to process all the data and make information out of it was too costly. Especially if you don't know where or what to look for.

Today, compute power and storage capacity are readily available. Opening opportunities for new business ventures and create smart solutions allowing us to do anything from anywhere by a single swipe. The progress is good but comes with an immense challenge. Keep data safe, accessible for those that are legitimate and protect it from unauthorized access that might jeopardize our privacy and harm our digital as well as our physical lives.

But what if sensitive data of you as is person is breached due to an uncareful action or lack of action by your employer?

I have nothing to hide

That is the most probable answer you get when you speak with non-privacy / security people. Though, when a breach occurs it always seems there is more out there than you've ever thought of. It remains difficult for people to comprehend data breach. Today it is focused on privacy in many discussions, it is important but as an organisation you don't make a lot of money by compliance, you avoid paying money. In many organisations it remains difficult to understand the true value of the data their sitting on, let alone to identify the so called "crown jewels". Those "crown jewels" could be your secret recipe, image you find the recipe from the leading soda company or the leading candy company.

What happens with the person made accountable for it, or being held responsible when that would occur?

In some past cases, people were threated to death, blackmailed, lost their jobs, income, house etc… The list of misery can be quite long and painful. If you're a CISO (the highest in command regarding cyber security activities in an organisation) and you're held accountable for a data breach with significant impact, your career could be over in a matter of seconds. Even if you've always fought to get the budgets and you never did, even if you were standing on the barrier to defend the rights with all good intentions.

The risk of falling into depression, burn-out or even end with suicide is a reality if your professional life exposes you to significant adverse event with important coverage internally or externally. Such an event is responsible for more collateral damage, any one standing in the line of fire at that very moment potentially at stake.

Sometimes, employees leak data. Unintentional or on purpose, to get money, to give them a competitive edge because they would like to start their own company or switch to a competitor. The reasons are rife but if there is dishonest intention, money is more likely to be involved. As a consequence, if you get caught your career is over, instantly. But you might face prosecution, pay penalties and even go to jail. In stark contrast with the effects if you're a victim, it could harm your integrity because your message is ripped out of context and made available to a large audience within the organisation or even to the general public. Even worse, someone or somebody could intentionally use false data to make somebody look bad. Such an event creates serious pressure on an individual and the impact is often underestimated.

Creating sensible defence

Many organisations feel confident about their security posture, either because they've outsourced a lot and provide way too much trust in the provider or either they don't get the numbers right or the reporting is wrong. Whatever it is, cyber security and information security are not constant, the only constant they have is it changes constantly. Risk and risk scenario's might not change that often, the defence mechanisms required to remediate the risks often do as does the exposure factor.

Working from home on cloud services is different than working from an office, where data can only be accessed via a terminal in that geofenced office.

It is important that companies review the maturity of their security. Oftentimes they do, based on frameworks or methodologies. NIST, ISO 2700x or even COBIT 5 are acronyms you'll come across easily.

Paramount for success is a holistic approach, understand the given context, how the organisation works what their business strategy is for now and in the near future etc… Reviewing purely based on am I in compliance with one or the other framework is insufficient, since the focus is mostly on effectiveness and less on efficiency.

It is key to understand the dynamics between structures, processes and relational mechanisms (Prof. Dehaes Information Technology Governance Best Practices in Belgian Organisations 2006). Having structures in place such as a CISO, a security committee etc… and process to manage your security such as project management, incident management etc… is relatively easy to manage. Understanding the importance of a relational mechanism, the required interaction between people to make the magic work, is paramount to ensure that what is written down and expected is also executed as such. Successful security maturity is not only about hard skills, the soft skills are increasingly important to provide enough level of confidence to your staff in order to report cyber misconduct or detect anomalies faster. It is not about controlling your users. Ultimately, the goal is getting people on board with your strategy instead of imposing it upon an organisation.

Moving forward

It seems today security strategies emphasize on prevention, it almost is as if we're all addicted to those very expensive medicine called preventative tools. We need them, but they're not going to help us survive the battle. Understanding how data flows in an organisation and monitor deviations on what can be considered normal provides more insight in anomalies than the majority of the tools that prevent evil doing.

These prevention tools work like the anti-flu vaccine, by now you know it doesn't work for COVID19. It helps us to get (re)infected from passed flu's and that is very useful, so we remain in good shape in case something unknown comes along. In order to detect anomalies, we'll need beef up our knowledge about the normal behaviour, that can be user login time, location or even device characteristics. The same goes for data, about 20 years ago I was involved in building a SOC (Secure Operations Center). Of course, at the time we oblivious of that terminology. Since communication lines had limited bandwidth, we monitored it actively to avoid operators being disconnected. By doing so, we created unintentionally a good understanding of the how much data flowed from where to where and at what time, taking into account different time zones as we worked 24/7. That helped to detect someone stealing critical data from a sensitive data storage. Because the files where so big it triggered alarms because it was outside the normal hours of transferring big files and during a time were operators in a certain time zone were active. After a close investigation we identified an authorised user tried to steal the data, probably to use it for other purposes. Only to realise years later, we still need to do that, one way or another. Perhaps not monitoring bandwidth at first, but understanding why machines speak with each other and is that expected outside business hours for example? If we get detection right, and we keep the usual evil out with our prevention tools. We've time left to focus on incident management.

Surviving the aftermath

Surviving, staying in good health and keep your senses together after a serious breach is extremely difficult as a security professional. The overwhelming media attention requires specialized communication, and transparency is key to success. Companies that correctly communicate are likely to suffer less financial and reputational impact after a breach. Integrating more controls in the wake of an incident requires full transparency towards employees to get them on board and support it.

Constructing a virtual castle is a strategy with a limited future and reduced capabilities, it is time to deploy knights. Your cyber knights are regular employees, once they understand that breaching security does not necessarily lead repercussion they'll come forward.

The problem with cybersecurity is that board members and executives only recognize it when it has failed. If you do everything right and you avoid severe breaches your business case is sometimes questioned. That is the nature of cybersecurity, when it works you don't see it.

The time has come to put CISOs on the decision makers' table, that the CISO learns business lingo and that other people in the business have a basic understanding of cybersecurity. For decades boards denied their dependence on technology, take it way and they'll come out quickly to say that it needs to be put back asap.

Information and technology are the lifeblood of a modern organisation. A CISO with business acumen is the one with the highest chance of being heard. Business leaders and board members valuing technology and advice from experts are the ones with the highest chance of getting a CISO with business acumen.

Rather than opposing one another, the solutions is to start working clever together.

Conclusion and recommendations

While solutions and strategies for minimizing data breaches continue to evolve, so too should the response and support given to those tasked with dealing with an incident. If an organization wants to give their staff flexibility and work remotely – especially with the rise of cloud services – then it needs to educate its employees on how to do so responsibly.

Keeping corporate data safe – no matter where it is being accessed – is always a top priority. It is clear that the impact on staff is hugely varied, but that the effects can be severe and long-lasting. As well as minimizing the impact on the business, enterprises and SMBs alike need to put measures in place to ensure the well-being and success of their staff.

"First of all, it's important to take a complex approach to improving cybersecurity in a company. Along with technical steps, organizations should improve business processes, implement effective management, working conditions and keep employees motivated. Otherwise pouring huge amounts of money into IT security doesn't help a company achieve its goals. It is like to treat only the symptoms of a disease, when the causes lie much deeper".

"Then, to build a safe environment for employees so they feel comfortable about cybersecurity risks, it is important to explain these risks to them, the consequences and also their responsibility to monitor their own actions in a digital environment. A company should also have dedicated rules regarding what should and shouldn't be done if an incident happens — whether that is because of an employee's mistake or an attack. A proper investigation should be done in advance of taking any disciplinary actions," adds Andrey Evdokimov.

From employees' perspective, there is also a way to facilitate things in case of breach and maybe even prove yourself, Alena Reva says: **"When an incident happens, it is important for every employee to analyze why it happened and what they could or couldn't do to prevent it. Try not to get anxious and scared about being penalized for the problem you have something or nothing to do with.**

"It's much more important to offer help and support in fixing the problem, figure out what damage is done and how that could be resolved. Being proactive to show the company management that you care about the business and you're working hard to help it to improve the situation will always work in your favor. It is even better, if you can learn from the situation and suggest improvements to processes to ensure that a similar breach will never happen again."

The following steps can help organizations mitigate cyberthreats and keep the impact of a breach on staff to a minimum:

- Explain to employees how following simple rules can help a company avoid cybersecurity incidents and the potential consequences via training courses, such as Kaspersky Automated Security Awareness Platform.

- Create a corporate culture where all employees, no matter which department they work in, understand the importance of cybersecurity. Teach them how cybersecurity incidents can occur and what the potential consequences of a successful attack could be for both the organization and themselves. Kaspersky Incident Communications training helps to upskill Corporate Communications teams to operate optimally during a cyberattack.

- Educate staff on the importance of carrying out tasks through authorized cloud services. Explain to them what services and tools are available and how they can obtain those that are not on their organization's approved list of applications. This should help decrease the risk of shadow IT when employees use services bypassing approval with corporate IT.

- Introduce an anti-crisis or incident response plan to help employees prepare, just in case the worst happens. This means staff respond quickly and effectively when a breach occurs without feeling additional stress or confusion.

- If a breach occurs, focus on properly investigating the causes and consequences instead of just searching for any guilty staff. This gives a clear understanding of measures that will help to avoid such incidents in future and maintain a trustful environment inside an organization.

- Invest in a verified and high-quality endpoint protection solution, such as Kaspersky Endpoint Security Cloud, that provides proven endpoint protection from the cloud, while helping control connections to cloud services. By combining cybersecurity training about the latest threat developments, with effective products and policies, organizations can make working life much more comfortable for their valued employees.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com/

www.kaspersky.com

kaspersky