From data boom to data doom: the risks and rewards of protecting personal data

Kaspersky Lab
2018

Contents

Introduction

We are living in a data boom: when it comes to running targeted and effective marketing campaigns, businesses naturally want to have databases flooded with information about their most loyal customers. And when it comes to running a business efficiently, it makes sense to keep the personal details of your employees, how much you pay them, and where they live, on file.

So, data is unavoidable in business today, right?

But at what point does all of this personal information become a risk? A risk to an individual's privacy, and also a risk to the company involved?

Data breaches have, for a long time, damaged companies and individuals alike. Recent examples can be seen in the Ticketmaster data breach, which put the login information, payment data, addresses, names and telephone numbers of 40,000 people at risk, and also in the already infamous Equifax breach, which lost the data of 145 million US citizens. Not only do breaches involve the involuntary spread of private information, causing harm to individuals, they result in serious financial and reputational damage to businesses too.

It's this issue that the General Data Protection Regulation (GDPR) has tried to address – by providing businesses with strict guidelines for dealing with the personally identifiable information (PII) of data subjects.

The GDPR is designed to enforce the protection of personal information. To stop businesses from misusing private data, and thus to stem the rapid flow of damaging data breaches that the business community has witnessed in recent years.

Is this, and the other data protection measures currently implemented by businesses, enough to stop the data boom from signaling data doom? At Kaspersky Lab, we've conducted a study into the state of data protection to find out more.

We discovered that the vast majority of businesses collect and store both customer and employee PII, and that over half **(61%)** expect the volume of sensitive customer data they store to increase in the next year.

With trends like mobility and cloud making waves in business, around **20%** of sensitive customer and corporate data now resides outside the corporate perimeter. With some on public cloud infrastructure and some even on the personal devices of employees, it's becoming extremely difficult to keep data under control.

Despite the fact that data is increasingly at risk, there is a false sense of preparedness among the business community. **72%** of SMBs consider themselves well, or even perfectly, equipped for a data breach, yet only **25%** can confirm that they have fully addressed the requirements for data protection as outlined by the GDPR, and **46%** of large enterprises (**42%** of SMBs) worldwide have experienced one or more data breaches.

And we discovered that data breaches, in this new landscape of strict compliance measures, are resulting in more than 'just' the exposure of PII, damaging financial implications and reputational harm. Breaches are also resulting in job losses at all levels of the command chain.

While businesses rate data protection as their top worry related to information security, the results of our study suggest that more needs to be done. Only with effective measures at hand, can businesses protect themselves and individuals from the threat of data doom.

Methodology

The Kaspersky Lab Global Corporate IT Security Risks Survey is an annual study into the state of IT security within organizations across the world. It is now in its 8th year and builds upon findings in the previous year.

A total of

5,878

interviews took place in 29 countries

Companies of different sizes – including very small businesses with 1-49 staff members, SMBs with 50-999 employees and major corporations/enterprises with over 1,000 employees. Fieldwork was completed in March-April 2018.

Key findings

- Sensitive data is flooding the corporate world - **88%** of businesses are already collecting and storing their customers' PII, and **86%** collect and store employee PII;

- One-in-three **(31%)** global businesses store data protected by the strict confines of the GDPR;

- This data is becoming more difficult to control - **20%** of sensitive customer and corporate data resides outside the corporate perimeter;

- There is a sense of preparedness for dealing with data breaches, with **72%** considering themselves well, or even perfectly, equipped for this sort of incident despite new legislation for data protection on the horizon;

- Moreover, **46%** of large enterprise (**42%** of SMBs) worldwide have had one or more data breaches, of which in two-fifths of cases, customer PII was affected (**41%** for SMBs and **40%** for enterprises);

- Data breaches result in job losses. Almost one-in-three (**31%**) data breaches have led to people losing their jobs and among these in **29%** of SMBs and **27%** of enterprises, it's senior non-IT employees that were laid off;

- One of the most common responses to a data breach is for businesses to enforce formal rules within their organizations, with **33%** of SMBs and **38%** of enterprises applying additional policies and requirements after an incident;

- More needs to be done. Internal and external audits, cybersecurity awareness training and a reliable security solution are all part of a holistic approach to data protection.

```
        mirror_mod.use_x = False
        mirror_mod.use_y = True
        mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
        mirror_mod.use_x = False
        mirror_mod.use_y = False
        mirror_mod.use_z = True

        #selection at the end -add back the deselected mirror modifier object
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
        #mirror_ob.select = 0
```

Personal data: it's everyone's business

Sensitive data is everywhere…

According to our research, **88%** of businesses collect and store their customers' PII, and **86%** collect and store employee PII. This, of course, is natural behavior for many: after all, how can you run a business without your customer contact details, and how can you pay your staff without their bank account information?

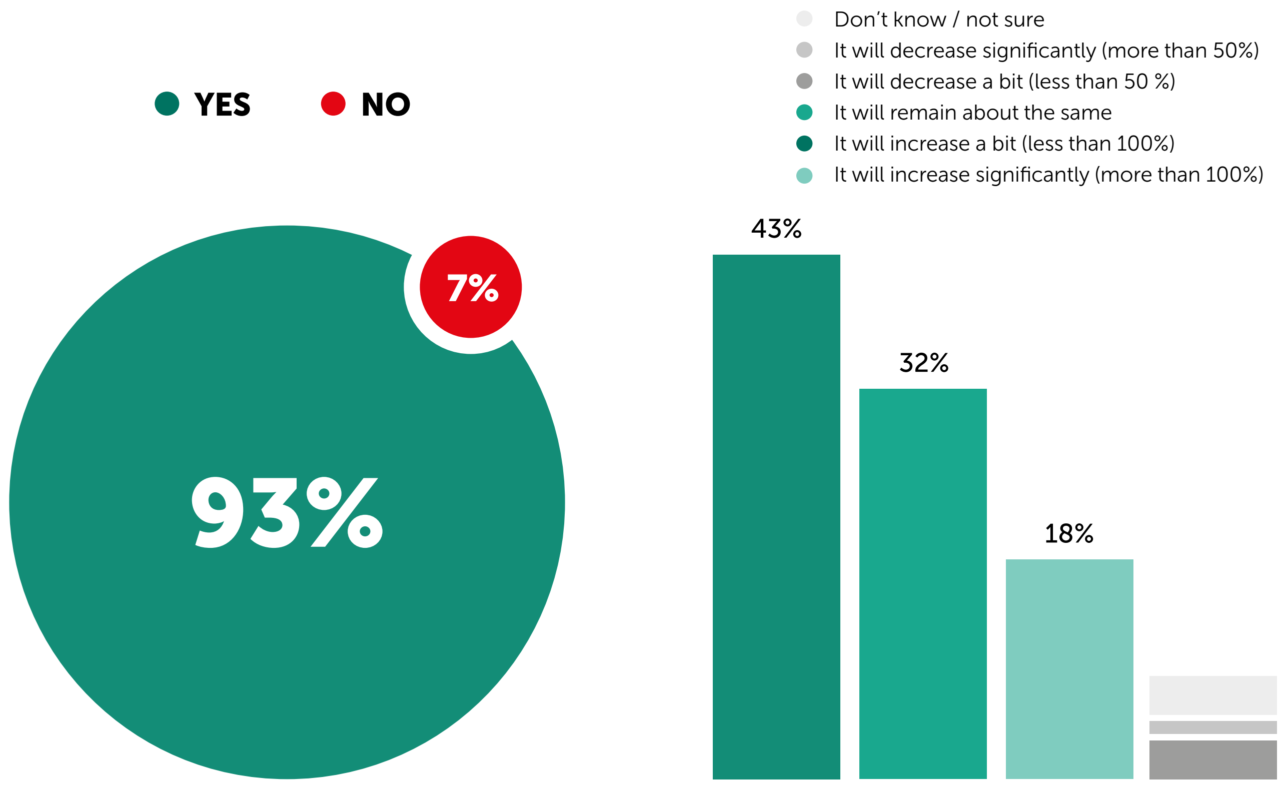
Nevertheless, in today's increasingly complex environment, storing personal information comes with breach and compliance risks.

And these risks are growing - **61%** expect the volume of sensitive customer data they store to increase in the next year. In addition, one-in-three global businesses store data protected by the strict confines of the GDPR (**31%** of businesses globally admit that they store personal data of EU citizens). Misuse this data, or store it insecurely, and businesses could face harsh and damaging fines. For example, severe financial penalties apply for a breach of the GDPR – up to **4%** of annual global turnover or up to €20 million (whichever is greater).

STORING SENSITIVE CUSTOMER DATA

Businesses storing some form of sensitive customer information

How the volume stored will change



Base: 5,878 all businesses

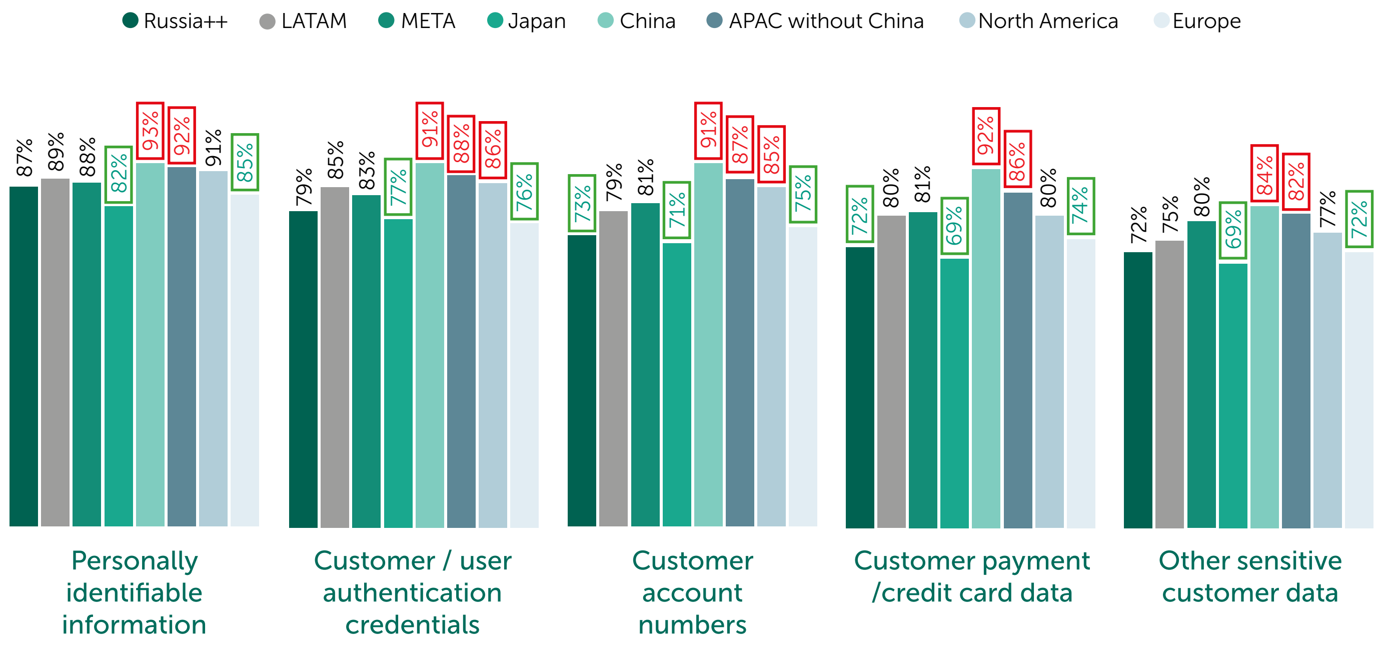
Base: 5,445 all businesses storing sensitive customer data

Table: Percentage of businesses storing sensitive customer information

Almost all businesses store sensitive customer data, so let's take a closer look at what sort of data is being kept by corporations, and how.

Over three-quarters of businesses store data such as customer authentication credentials **(82%)**, account numbers **(80%)** or credit card details **(78%)**. There are some regional differences worth mentioning here – with businesses in China and APAC consistently more likely to store sensitive customer data, and with significantly fewer businesses in Europe and Japan storing customer data of this kind.

WHAT CUSTOMER DATA IS BEING STORED
REGIONAL SPLIT



□ - Significantly more businesses store this in this region

□ - Significantly fewer businesses store this in this region

Base: 5,878 all businesses in 2018

Table: What customer data is stored by businesses – regional split

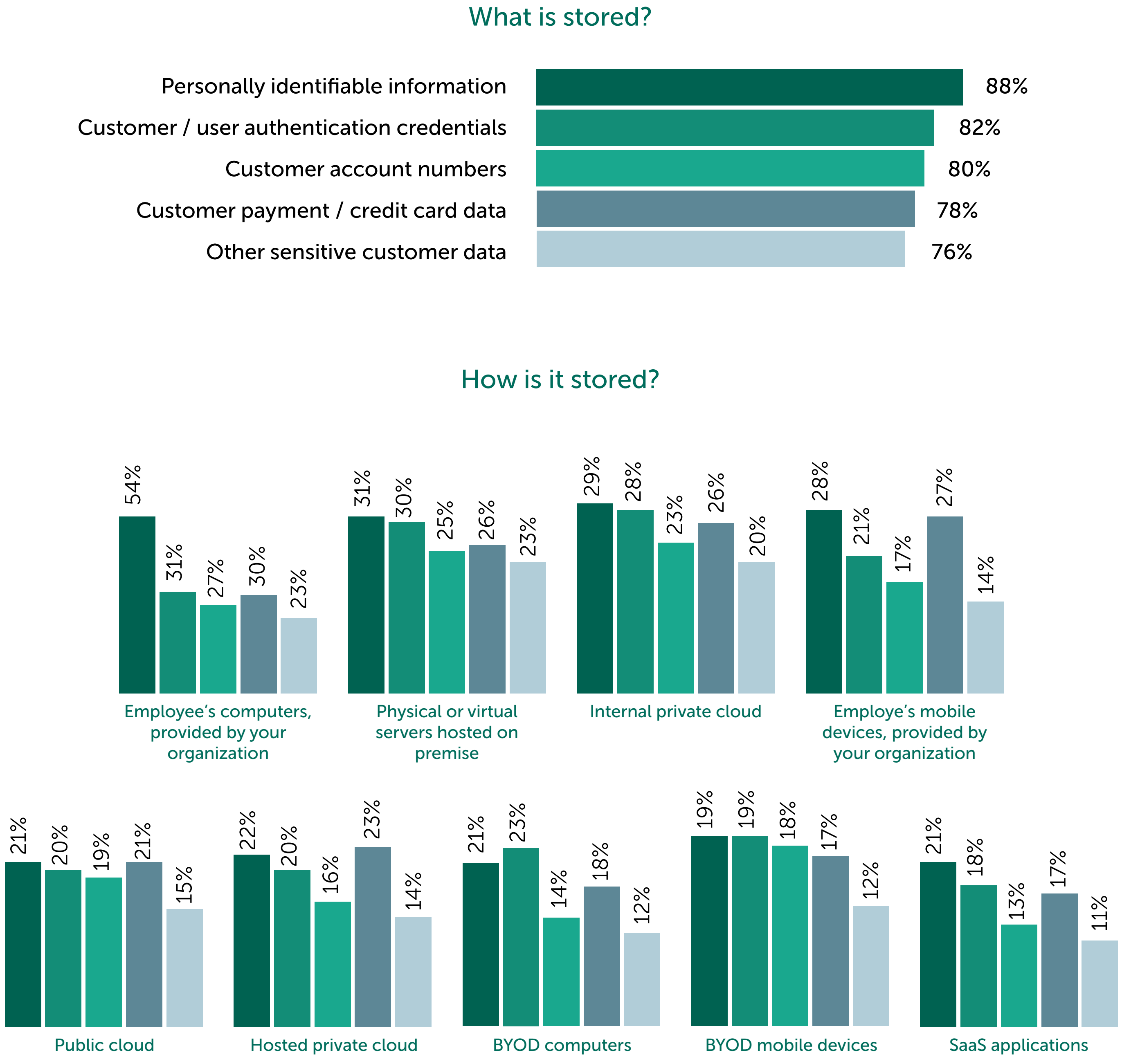
...and it's difficult to manage

So sensitive data is everywhere, but controlling this data and keeping it safe is a constant and evolving issue for businesses.

This challenge is made more complex by the fact that approximately **20%** of sensitive customer and corporate data resides outside the corporate perimeter (for example in public cloud, BYOD devices and in SaaS applications). This creates additional security risks because this data becomes harder to control, may be subject to third party security defects, or may end up at the mercy of forgetful, neglectful or even frustrated employees.

WHAT CUSTOMER DATA IS BEING STORED AND HOW?

ALMOST ALL BUSINESSES STORE SENSITIVE CUSTOMER DATA


What is stored?

How is it stored?

Base: 5,878 all businesses in 2018

Table: What customer data is stored by businesses and how

For example, almost one-in-five **(17%)** admitted in our research that they have customer credit card data on employee BYOD devices - making this information vulnerable should that device not be within control of the organization in question, should an employee leave the firm, or should the device be lost or intercepted.

Furthermore, around a fifth **(21%)** of businesses store PII in the public cloud, and the same number (also **21%**) store this type of data in SaaS applications, making it vulnerable to the security flaws of these third parties.

The scramble to protect data

Data protection: the security concern to trump all others

Perhaps because they are aware of all of the sensitive data in their control, businesses rate data protection as the top business worry related to information security, a trend which continues from 2017.

Among the SMB and enterprise community for example, **64%** consider data protection to be the most concerning IT security related business issue, naming data loss/exposure due to targeted attacks as their biggest fear **(30%)**. The second most concerning IT security related business issue is security around cloud infrastructure adoption – a concern that was second place in 2017 too.

TOP IT CONCERNS FOR SMB+

	Most concerning IT security related business issues	Top 3 security challenges related to each business issue		Rank of concern	
Data protection	**64%**	Data loss/exposure due to targeted attacks	30%	**1st**	**1st**
		Electronic leakage of data from internal systems	27%		
		Physical loss of devices or media containing data	24%		
Security issues of cloud infrastructure adoption and business process outsourcing	**43%**	Incidents affecting IT infrastructure hosted by a third party	17%	**2nd**	**2nd**
		Incidents affecting third party cloud services we use	14%		
		Incidents affecting suppliers that we share data with	14%		
Ensuring compliance of staff with security policies and regulatory requirements	**42%**	Inappropriate IT resource use by employees	21%	**5th**	↑ **3rd**
		Time and cost of enforcing employee security compliance	19%		
		Fines for not maintaining compliance with security regulations	13%		
Relationships with partners / customers	**41%**	N/A		**6th**	↑ **4th**
Business continuity	**40%**	Viruses & malware	15%	**3rd**	↓ **5th**
		Loss of access to internal services	14%		
		Loss of access to customer-facing services	13%		
Cost of securing increasingly complex technology environments	**38%**	Identifying / remedying vulnerabilities in IT systems we use	18%	**4th**	↓ **6th**
		Managing security across different computing platforms	15%		
		Incidents involving non-computing, connected devices	13%		
Security issues of mobile devices and BYOD trends	**32%**	Managing security of users' own devices in the workplace	14%	**7th**	**7th**
		Inappropriate sharing of data via mobile devices	14%		
		Physical loss of mobile devices exposing the organization to risk	13%		

Base: 4,039 businesses with 50+ employees

Table: Top SMB+ IT concerns

Although data protection comes out on top of the list of IT concerns for businesses, there are significant regional differences. Significantly more businesses in Russia **(75%)** see data protection as a concern, compared to just **59%** of European businesses. Perhaps businesses in Europe are less concerned because they are already taking additional measures in light of the GDPR.

DATA PROTECTION CONCERN: REGIONAL SPLIT

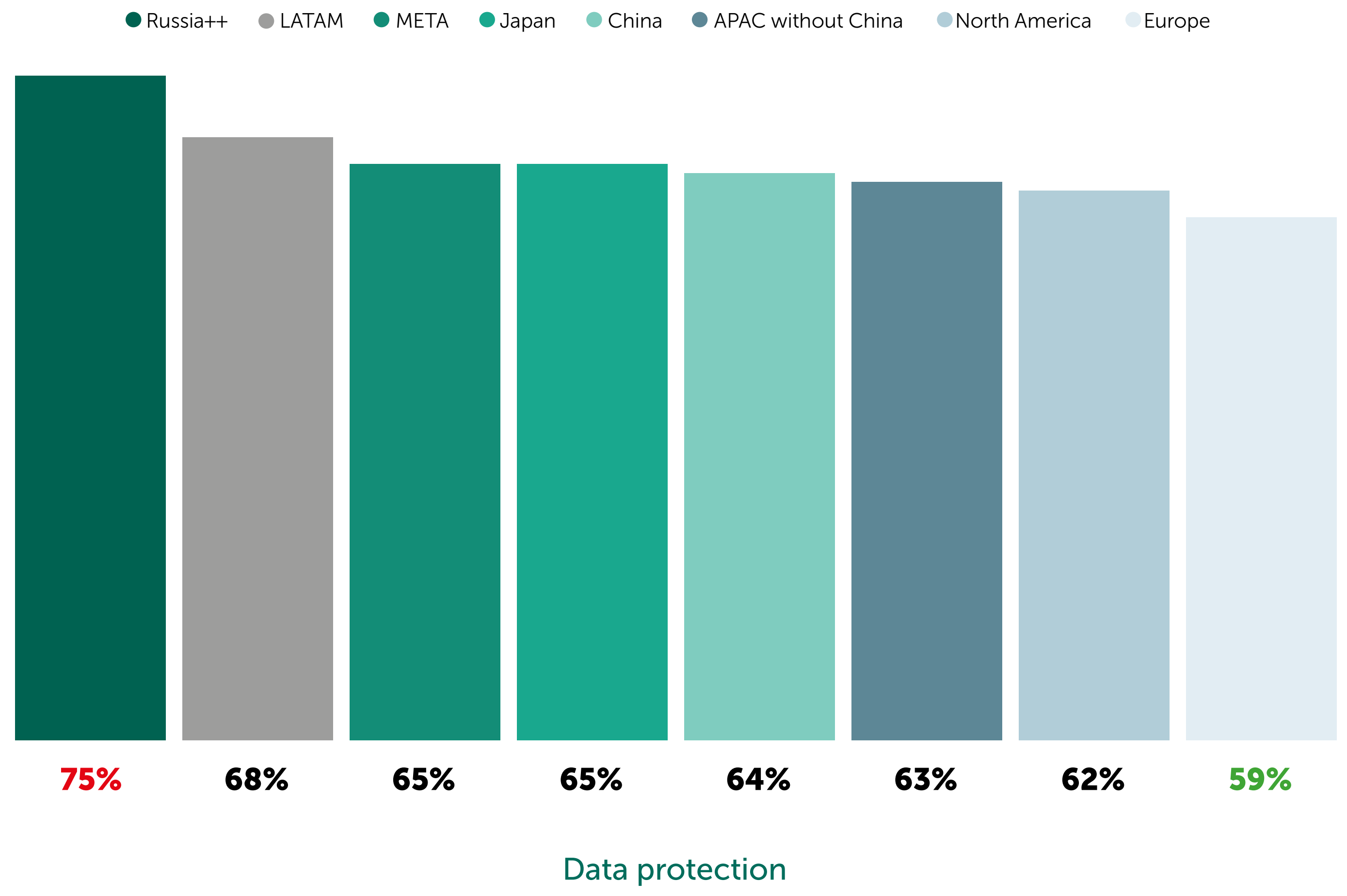


Table: Top SMB+ IT concerns – regional split

Still, businesses feel prepared

Data protection is certainly a concern among the business community, but delving into the research further, we can see a degree of confidence among businesses too.

There is a sense of preparedness for dealing with data breaches, with **72%** of SMBs considering themselves well, or even perfectly, equipped in terms of data protection and compliance. And what's more, this figure is even higher among large enterprises **(78%**).

Is it false confidence?

Well, our research tells us that **86%** of businesses have at least some form of data security and compliance policy in place. This may be helping them to feel ready, but there is certainly still more work to be done before data is truly protected in business.

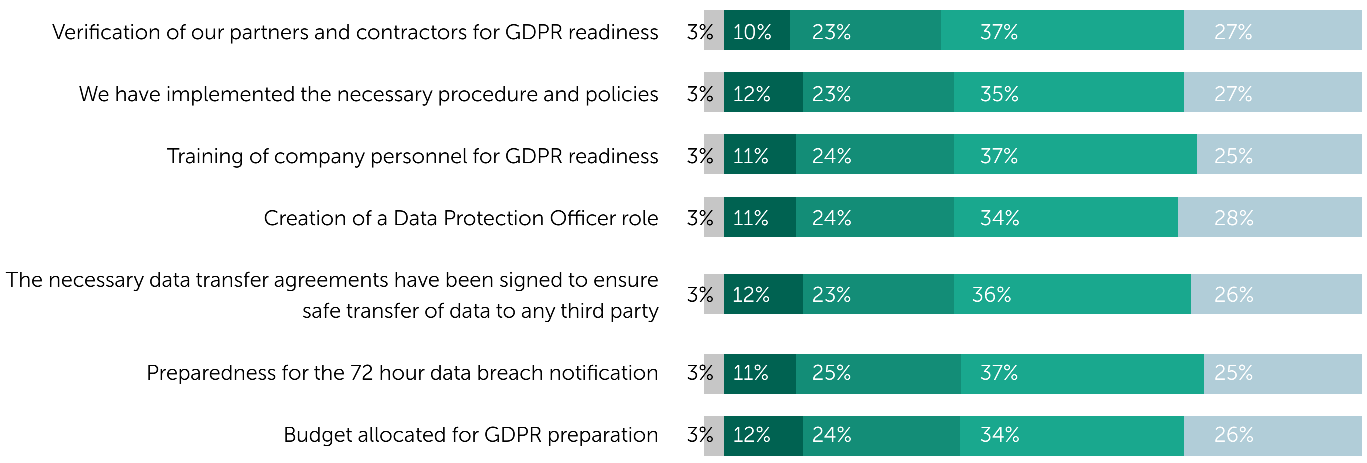
For example, just because a business has a privacy policy it's not guaranteed that data will in fact be handled properly. And, in terms of the GDPR, although **88%** of affected businesses know about the regulation, **41%** have identified at least one aspect of preparation that they have not even begun to address.

There's a need for security solutions that can protect data across the whole infrastructure – including cloud, devices, applications and more. There's also a need for cybersecurity awareness among IT staff and beyond, as more and more business units are now working with data, and thus need to understand how to keep it safe.

GDPR – HOW READY ARE BUSINESSES?

Many businesses are still a long way short of being ready for GDPR, with 41% identifying at least one aspect of preparation they have not even begun to address

● Don't know / not sure
● We have not begun to address this requirement
● We have plans to address this requirement, but have not started addressing it yet
● We are currently working on it
● We have fully met this requirement



Base: 1,591 all businesses storing personal data from residents of the European Union who are aware of GDPR

Table: Business readiness for the GDPR

VSBs, and businesses outside of Europe are the most likely to be lacking in their knowledge about the GDPR.

For example, **50%** of businesses that store sensitive customer information in Europe agreed they should, and do, know about the GDPR. But this drops to **25%** among Chinese businesses that store sensitive customer information, and **18%** among Russian businesses.

As many as **17%** of VSBs said they would be unable to notify the relevant authorities within 72-hours, should a data breach occur at their business. That's compared to just **7%** of enterprises, which are much more prepared to meet this crucial part of the GDPR compliance requirements.

Although the GDPR is a European regulation, crucially, it does impact any business that holds and stores EU citizen data, regardless of size, so we would have hoped to see higher levels of awareness and preparedness across the different regions and across different sized businesses.

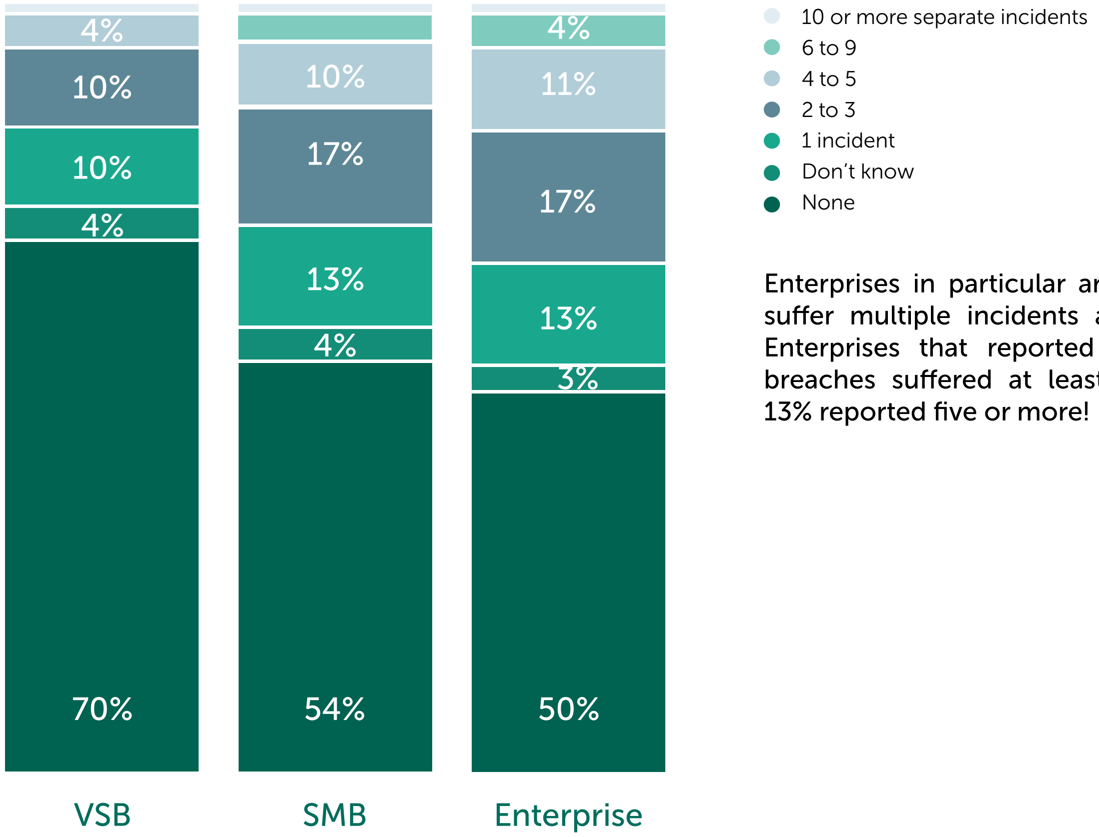
Data breaches and response: formal procedures and lost jobs

New regulations such as the GDPR are making the impact of a data breach more severe than ever – because of the damaging fines involved. So, let's take a look at data breach trends.

42% of businesses worldwide have had at least one data breach, of which in two-fifths of cases, customer PII was affected (**41%** for SMBs and **40%** for enterprises). After malware infection, the second most likely cause of a data breach is a business suffering from a targeted attack **(22%)**.

HOW MANY DATA BREACHES ARE HAPPENING?

DATA BREACHES AREN'T ONE OFF EVENTS. IN MOST CASES, WHERE ONE EVENT HAS OCCURRED IN A YEAR, MORE HAVE FOLLOWED



Enterprises in particular are likely to suffer multiple incidents as 68% of Enterprises that reported any data breaches suffered at least two and 13% reported five or more!

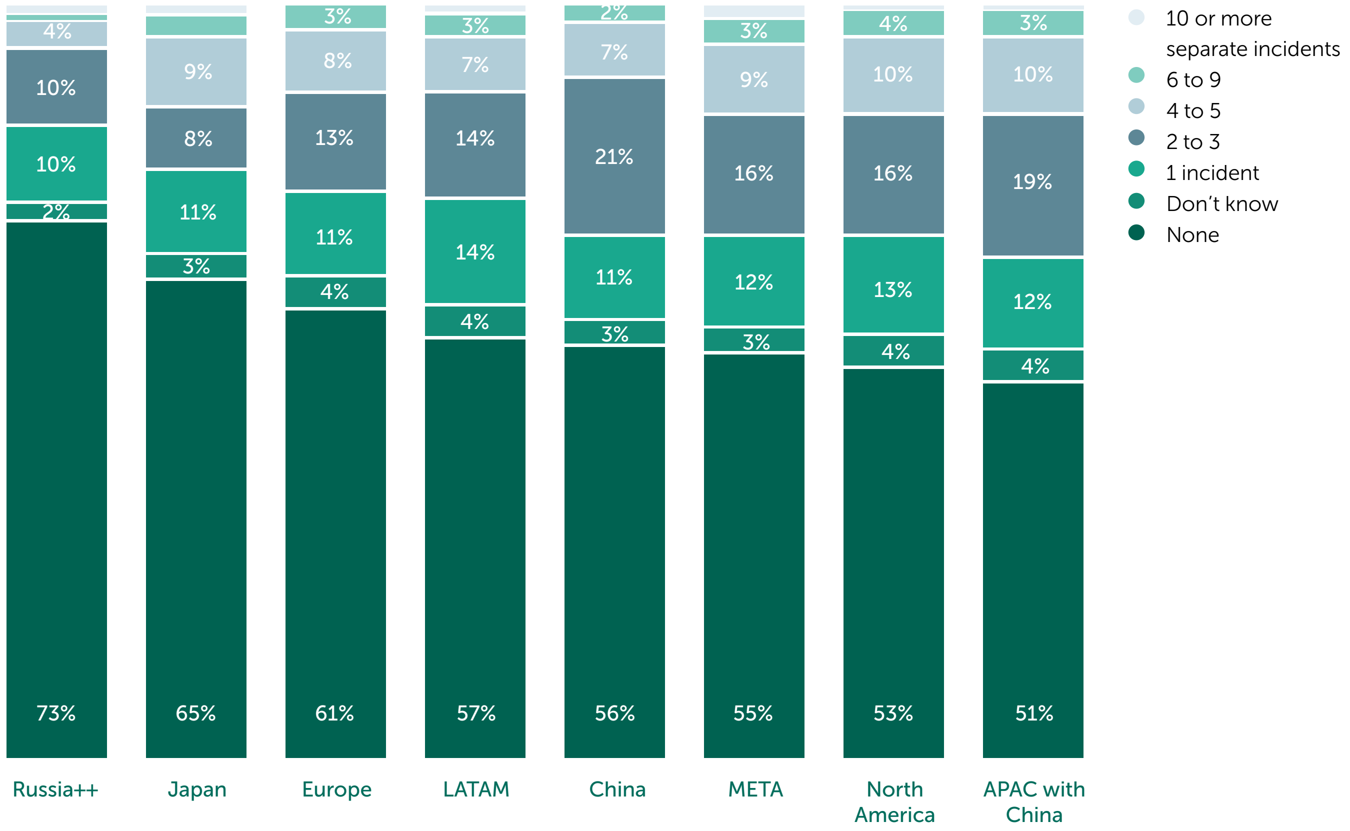
Base: 5,878 all respondents

Table: The number of data breaches across different sized businesses

Our study shows that data breaches aren't one off events. Often one breach is followed by another – for example, **68%** of enterprises that have suffered a breach admitted in our research that they have actually reported at least two breaches, and furthermore, businesses in North America are among the most likely to be affected.

HOW MANY DATA BREACHES ARE HAPPENING?

NORTH AMERICAN BUSINESSES ARE AMONG THE MOST AFFECTED BY DATA BREACHES



Base: 5,878 all respondents

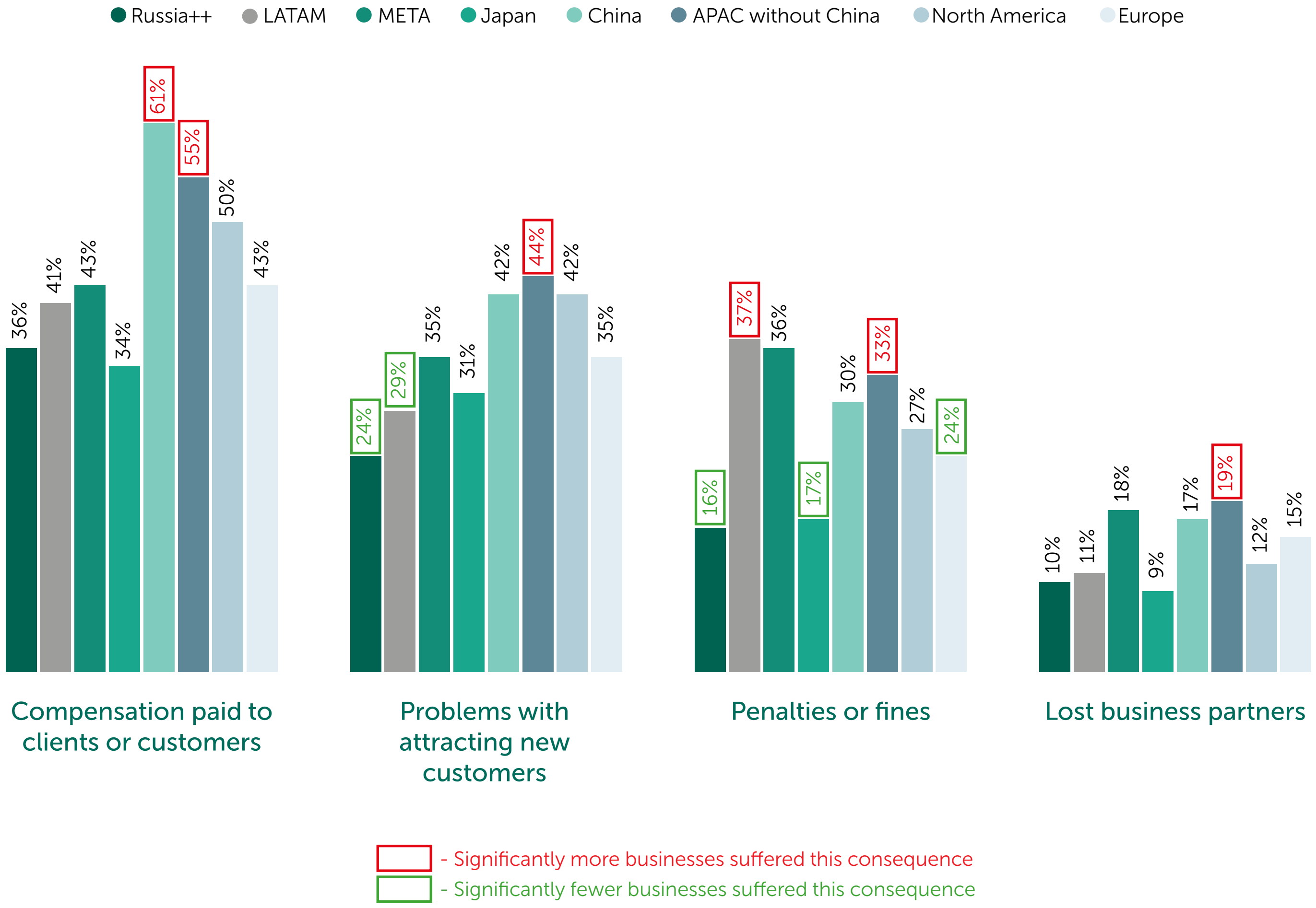
Table: The number of data breaches experienced by businesses across different regions

Data breaches happen – so what?

Data breaches have a big impact on the organizations affected. Overall, the average financial impact of data breaches on SMBs and enterprises has continued to rise over the last 12 months to $120K for SMBs (an increase from $88K in 2017) and to $1.23M for enterprises (from $992K in 2017).

Of those businesses in our study that have suffered from a data breach, **45%** of SMBs and **47%** of enterprises have had to pay compensation to the customers affected, over a third - **35%** and **38%** respectively - have reported problems attracting new customers, and over a quarter of SMBs **(27%)** and of enterprises **(31%)** have had to pay penalties and fines.

COMPENSATION AND FINES



Base: (1,062 SMBs and 863 Enterprises) all respondents from businesses with 50+ employees who experienced any data breaches

Table: Compensation and fines after a data breach

Looking at the consequences of a data breach, we can see some interesting comparisons across different regions. Businesses in China and APAC seem particularly vulnerable to having to pay compensation to clients or customers after a breach, whereas businesses in Russia, Japan and Europe are less likely to pay a fine after a breach.

Hold on a second – that's my job!

Data breaches don't just come with nasty fines, lost business, and hidden costs. They also result in job losses. Almost one-in-three **(31%)** data breaches have led to people losing their jobs and among these in **29%** of SMBs and **27%** of enterprises, it's senior non-IT employees that were laid off.

NON-FINANCIAL FALLOUT OF DATA BREACHES

ALMOST ONE IN THREE BREACHES RESULTS IN EMPLOYEES BEING LAID OFF

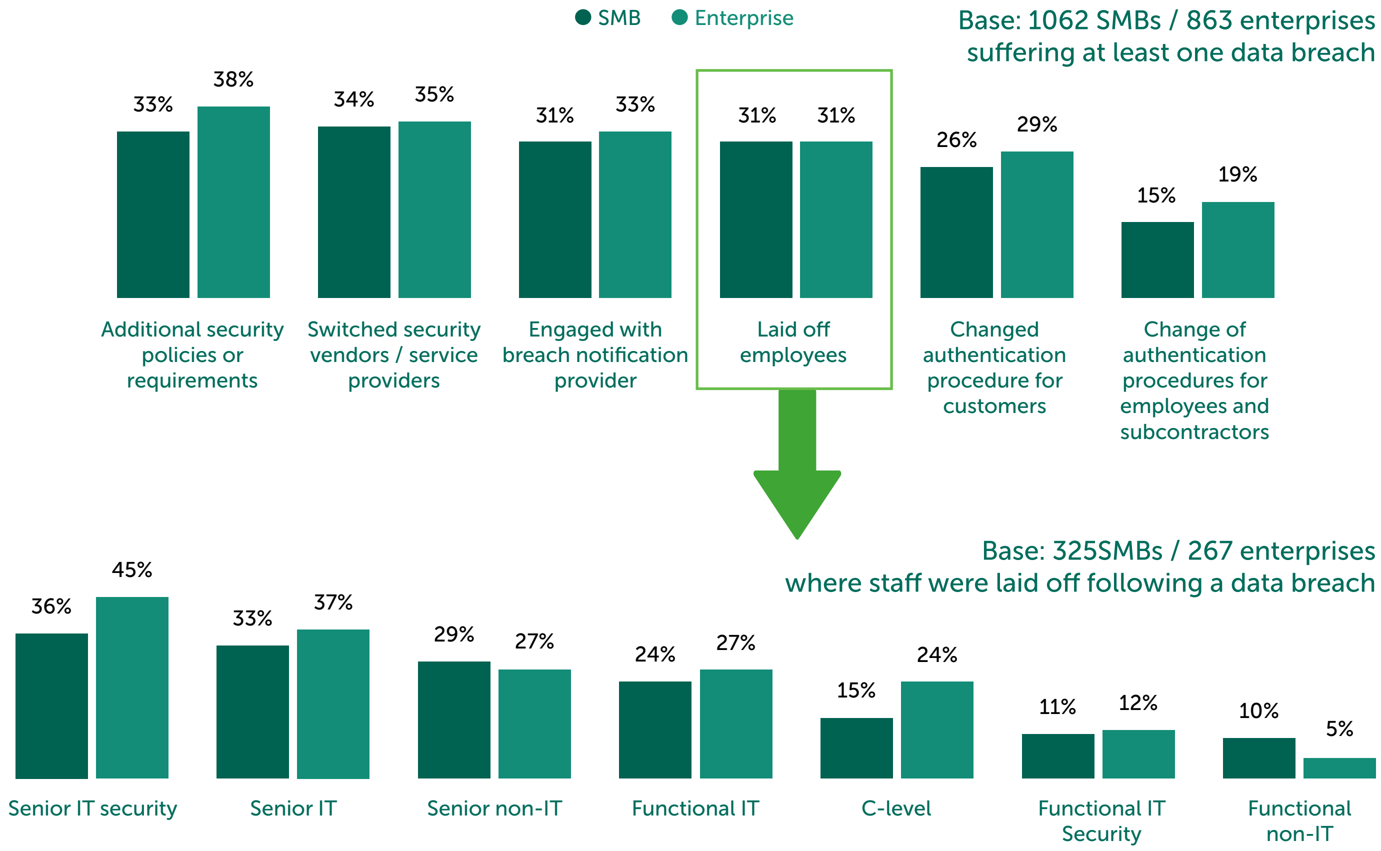


Table: Job losses as a result of a data breach

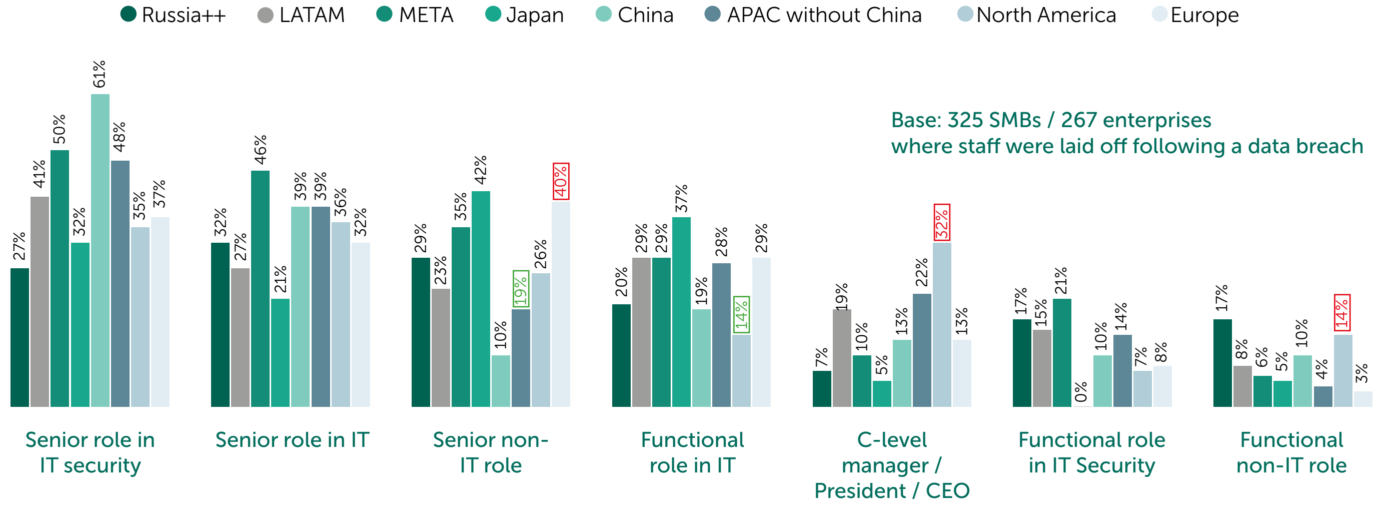


Table: Job losses as a result of a data breach, by region

In North America, a data breach is most likely to be blamed on the C-suite, with **32%** of breaches here resulting in a C-level manager/president/CEO losing their job compared to, say, **5%** in Japan. However, the statistics show an overwhelming number of senior IT security roles being laid off in China – making this the most likely job loss across the globe, following a data breach.

Finding out about a breach

HOW ARE DATA BREACHES DISCOVERED?

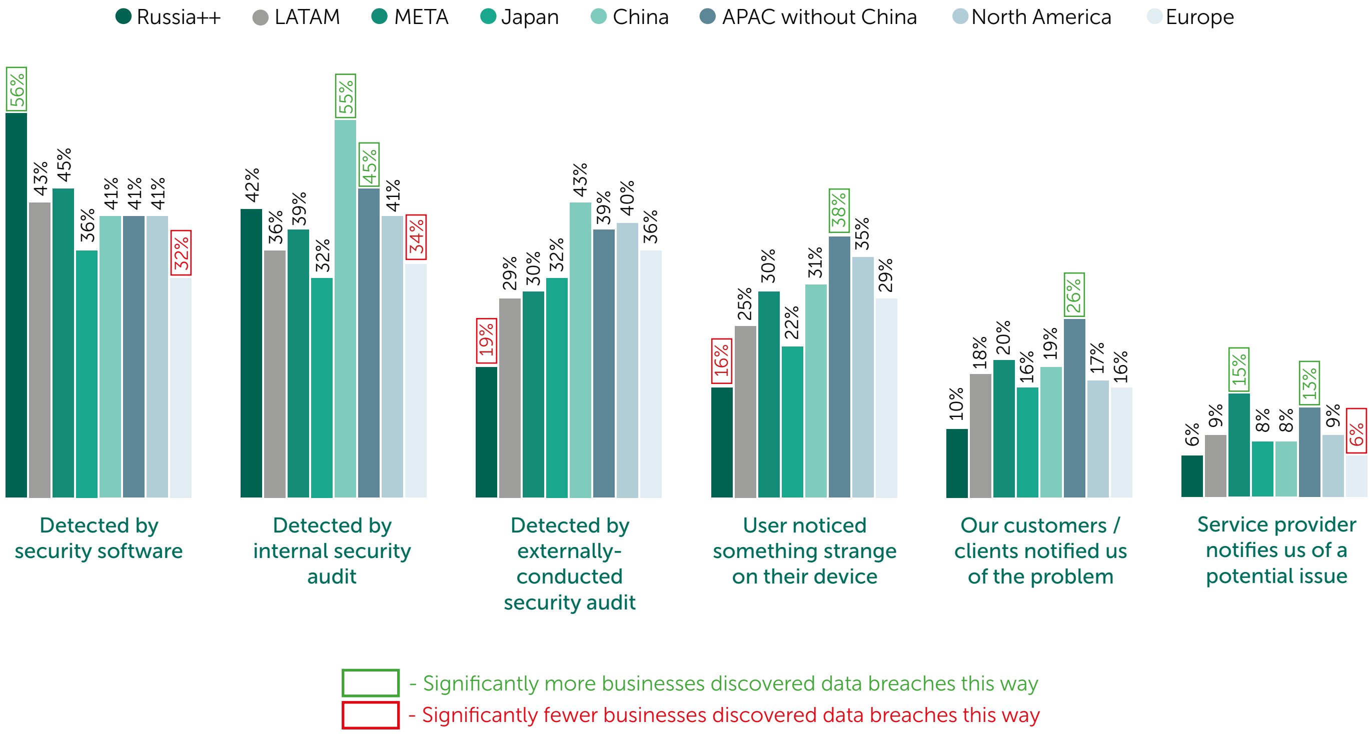


Table: Job losses as a result of a data breach, by region

Our research has found that data breaches are discovered in a variety of ways, but that security software and audits are a vital part of discovering a breach. For example, **56%** of breaches in Russia are detected by security software, dropping to **32%** in Europe. Meanwhile, internal security audits are most effective in China **(55%)** and other APAC countries **(45%)**.

What are businesses doing about it?

One of the most common responses to a data breach is for businesses to enforce formal rules within their organizations, with **33%** of SMBs and **38%** of enterprises applying additional policies and requirements after an incident. But worryingly, at **7%** of businesses, nothing changes after a breach.

It's important for the business community to remember that where sensitive data, and jobs are at risk, breaches require action.
Policies alone are not the answer and there is a clear need for businesses to invest in security audits, cybersecurity awareness training for staff, and comprehensive security solutions if they are to protect themselves and their data from harm.

Conclusion

Our study has demonstrated that the business world is brimming with personal and sensitive data. This data can bring rewards – but if it is not cared for effectively, it can also bring risks.

Many businesses, it seems, are on the cusp of data doom. Why? Because they are simply not protecting the data in their care effectively. This has two key implications: on the one hand it means that they are at risk of being found non-compliant with crucial new data protection measures such as the GDPR. And on the other hand, it means that they are at risk of experiencing a data breach that could not only damage their bottom line, but also impact their reputation and cause job losses in the process.

It's a dangerous time, but for businesses that want to take a more proactive approach to data protection, there are some simple and effective steps they can take.

Implementing the necessary GDPR procedures and policies, hiring a data protection officer, and ensuring that a data breach can be identified and reported within 72-hours are all crucial to GDPR compliance, but too few businesses have so far addressed these points. Likewise, having regular audits and deploying effective software will help mitigate the consequences, and reduce impact of data breaches.

Ultimately with so much sensitive data in business hands, it's time the business community stepped up to the challenge of data protection. For those that fail to do so, the data boom we are currently living in, might quickly turn into a time of data doom.