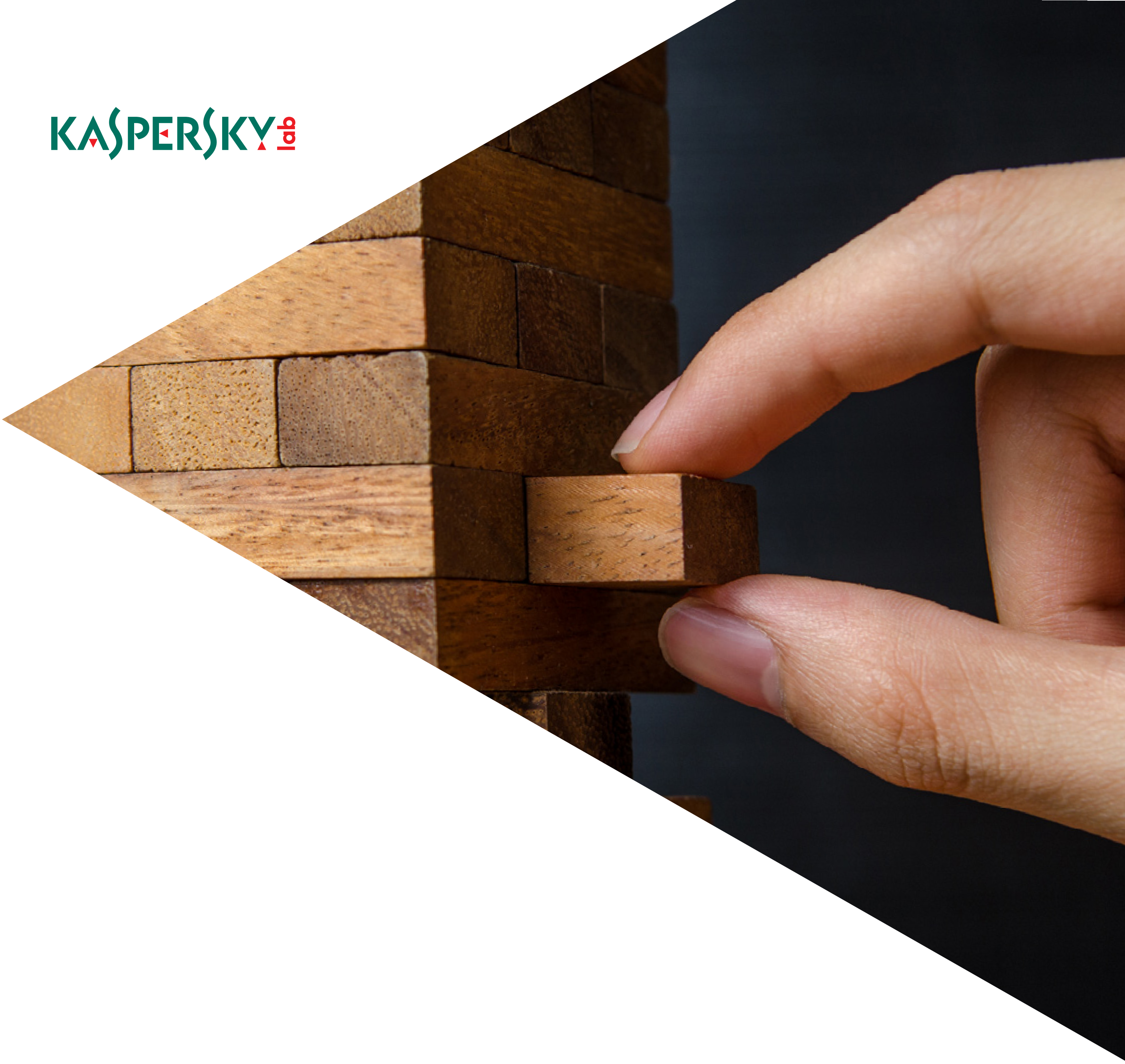


THE HUMAN FACTOR IN IT SECURITY

How Employees are Making Businesses Vulnerable from Within.

Introduction

Sometimes personnel may take cybersecurity requirements too lightly, leading to dramatic consequences for the organizations they work for.

In the recent WannaCry ransomware epidemic, the human factor played a major role in making businesses worldwide vulnerable. Two months after the disclosed vulnerabilities had been patched with a new update from Microsoft, many companies around the world still hadn't updated their systems. Several cases followed — with non-IT personnel being the weakest link: for example, employees with local administrator rights who disabled security solutions on their computers and let the infection spread from their computer onto the entire corporate network.

Switch off my computer and lose all these tabs in my browser? There's no way I'm doing that.
Windows Update
Remind me in:
10 minutes
Restart now
Postpone

Restart your computer to finish installing important updates

Windows can't update important files and services while the system is using them. Make sure to save your files before restarting.

So, what role do employees play in a business's fight against cybercrime? To answer this question Kaspersky Lab and B2B International have undertaken a study into over 5,000 businesses around the globe.

The results have been astounding. We've found that just over half of businesses (52%) believe they are at risk from within. Their staff, whether intentionally or through their own carelessness or lack of knowledge, are putting the businesses they work for at risk.

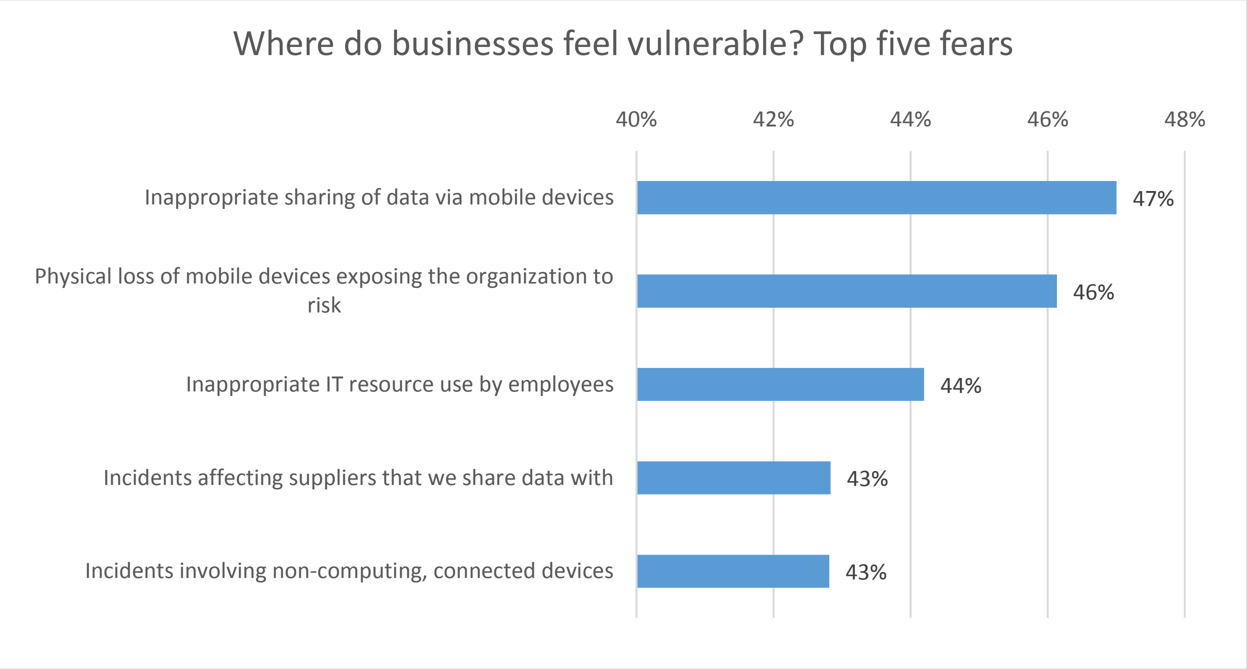
The following report investigates how and why this is happening – and what businesses can do to help protect themselves from their own employees.

The dangers of irresponsible and uninformed employees

At risk from within

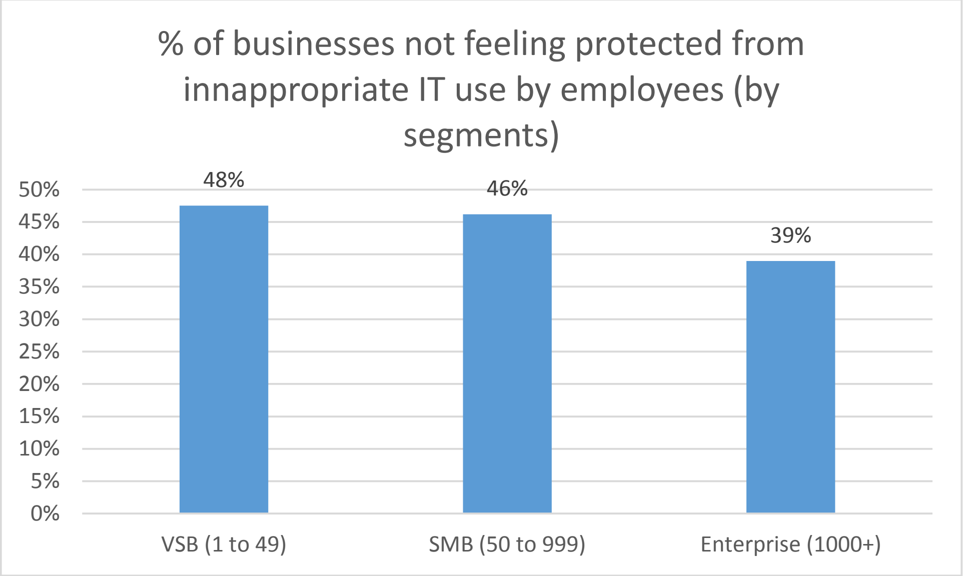
Against the backdrop of a complex and growing cyber threat landscape, where 57% of businesses now assume their IT security will become compromised, businesses are also waking up to the fact that one of the biggest chinks in their armor against cyberattack is their own employees. In fact, 52% of businesses admit that employees are their biggest weakness in IT security, with their careless actions putting business IT security strategy at risk.

The fear of being put at risk from within can be seen clearly in the fact that for businesses, the top three cybersecurity fears are all related to human factors and employee behavior. The table below shows that businesses are aware of how easy it is for employee/human error to impact their company's security. They worry most about employees sharing inappropriate data via mobile devices (47%), the physical loss of mobile devices exposing their company to risk (46%) and the use of inappropriate IT resources by employees (44%).



Source: IT Security Risks Survey 2017, global data

Taking a closer look at these findings, concerns about the inappropriate use of IT by employees vary considerably according to company size, with very small businesses (with 1-49 employees) feeling more at risk from this threat than enterprises with more than 1000 staff. This could be due to a number of factors including enterprises potentially having stricter policies in place, and more thorough training for staff on best practice. In addition, very small businesses possibly bestow employees with a greater degree of flexibility in terms of how they use business IT resources.



Source: IT Security Risks Survey 2017, global data

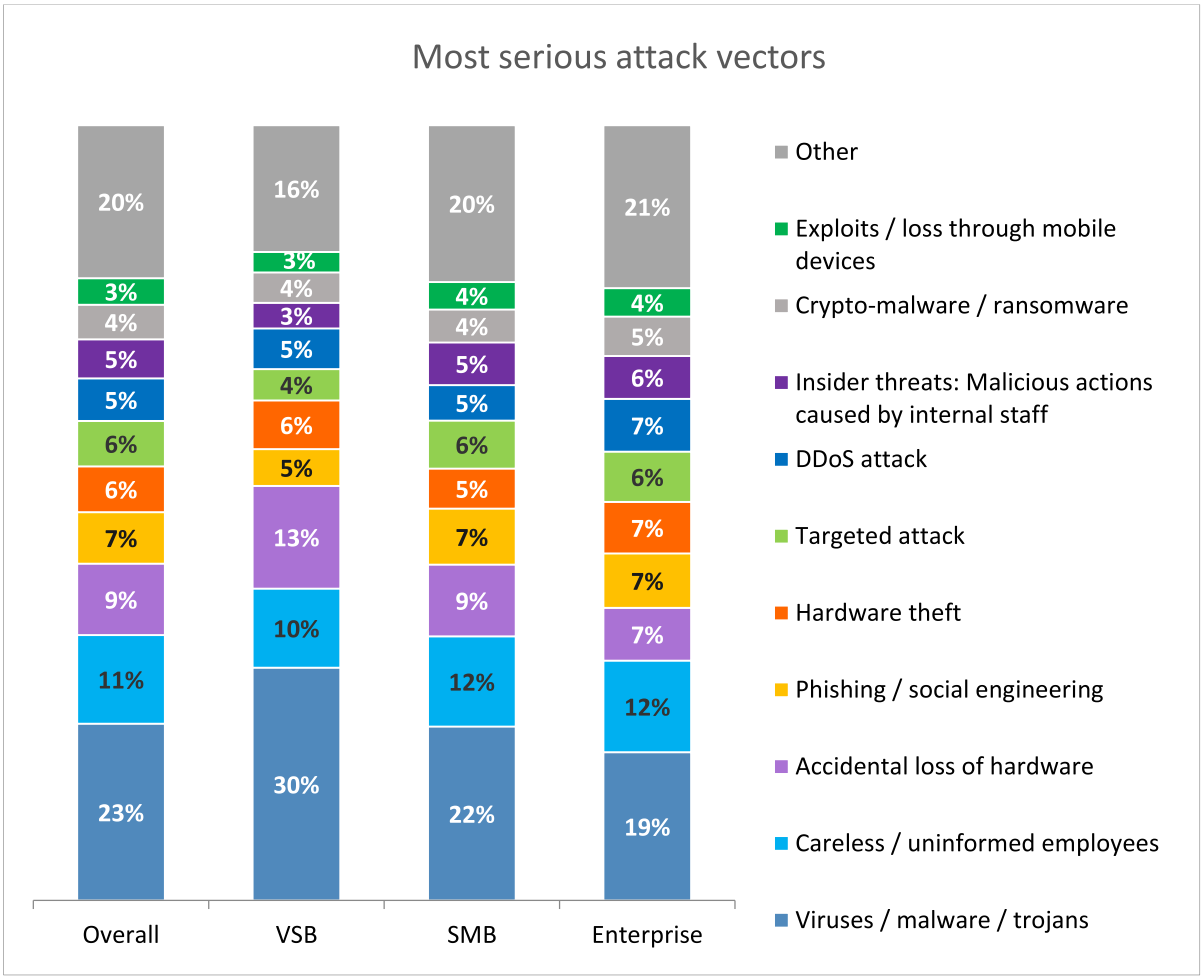
Employee actions lead to cybersecurity incidents

The findings of our study show us that businesses do indeed have good reason to be worried about employees contributing to cybersecurity risks. Staff may make mistakes that put their company's data or systems at risk – either because they are careless and accidently slip up – or even because they do not have the required training to teach them how to behave appropriately and to protect the business they work for.

Careless or uninformed staff, for example, are the second most likely cause of a serious security breach, second only to malware. In addition, in 46% of cybersecurity incidents in the last year, careless/ uniformed staff have contributed to the attack.

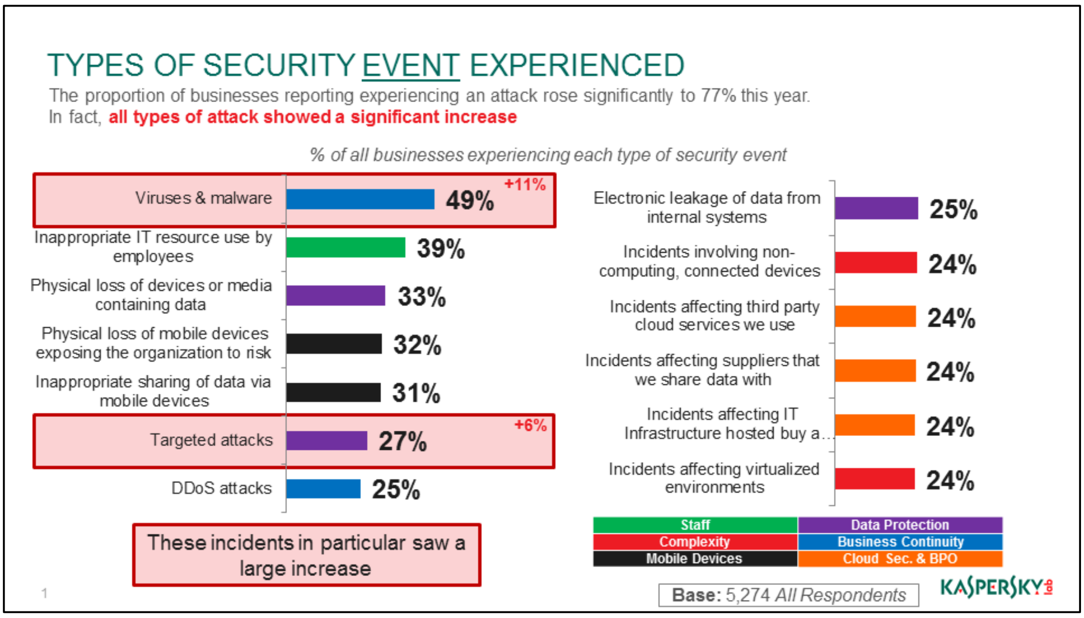
Human error on the part of staff is not the only 'attack vector' that businesses are falling victim to. In the last year internal staff have also caused security issues through malicious actions of their own, with 30% of security events in the last 12 months reportedly involving staff working against their own employers.

Among the businesses that faced cybersecurity incidents in the past 12 months, one-in-ten (11%) the most serious types of incidents involved careless employees.



Source: IT Security Risks Survey 2017, global data

Employee carelessness and phishing/social engineering were major contributing factors for malware and targeted attacks; attack types, which, incidentally, have also demonstrated the largest increase in the last year.



TYPES OF SECURITY EVENT EXPERIENCED

The proportion of businesses reporting experiencing an attack rose significantly to 77% this year.
In fact, **all types of attack showed a significant increase**

% of all businesses experiencing each type of security event

These incidents in particular saw a large increase

Base: 5,274 *All Respondents*

Source: IT Security Risks Survey 2017, global data

As many as 49% of businesses worldwide reported being attacked by viruses and malware this year, an 11% increase compared to 2016 results. And, of those that experienced virus and malware incidents, just over half (53%) of these consider careless/ uninformed employees to be a top contributing factor and over a third (36%) consider phishing/ social engineering to have contributed to the threat.

Viruses & malware

	2017 (Y2Y dynamics)
% of businesses that reported incidents	49 (11% increase from 2016)
Top contributing factors	1. Careless/ uninformed employees (53%) 2. Accidental loss of hardware (38%) 3. Phishing/ social engineering (36%)

Source: IT Security Risks Survey 2017, global data

Likewise, more than one-in-four (27%) businesses have experienced targeted attacks this year, a 6% increase on last year. Of these attacked businesses, over a quarter (28%) believe phishing/ social engineering contributed to the attack.

Targeted attacks

	2017 (Y2Y dynamics)
% of businesses that reported incidents	27 (6% increase from 2016)
Top contributing factors	1. Viruses/ malware (49%) 2. Exploits/ loss through mobile devices (30%) 3. Phishing/ social engineering (28%)

Source: IT Security Risks Survey 2017, global data

If these attack scenarios are increasing, and employees are contributing to them (whether innocently or willingly) businesses need to do more to reduce the dangers they are exposed to and better protect their systems.

Hide and seek

When security incidents happen at a business, it’s important that employees are on hand to either spot the breach, or mitigate the risks. After all, while employees can pose a risk to companies (as seen in our findings thus far), they also have an important role to play in helping protect the companies they work for.

However, employees don't always take action when their company is hit by a security incident. In fact, in 40% of businesses around the world, employees hide an incident when it happens.

Hiding an incident may lead to dramatic consequences, increasing the damage caused. One unreported event can even lead to an extensive breach of the organization's entire infrastructure, as explained by an employee from a consulting company that experienced such an incident:

"There was a lady at our company who hated her corporate laptop. She was in the legal department and always had several documents open and being edited at the same time. The computers we used then were old and could not always keep up with the workload. So, every time her laptop experienced a bug and she lost all of the changes to her documents, she ran into the IT department yelling and screaming.

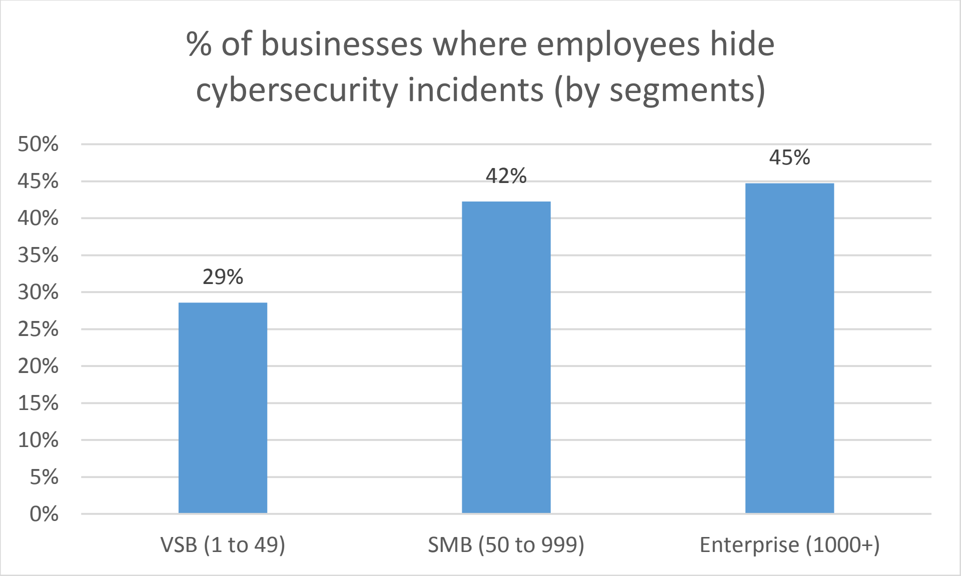
Enough was enough. She decided one day to bring her personal laptop in from home and argued her case to use it instead of the company equipment. Management decided to let her work from her own computer with local administrator rights.

Several weeks later, she got a cryptor upon opening an attachment from an obviously fake email. The files on the laptop were encrypted with a $300 ransom demand. All personal photos, videos and also important legal documents she'd been working for the past few weeks were affected and potentially irretrievable. The lady considered her options for a few days. She didn't want her corporate laptop back and couldn't risk losing personal files as well as a month's worth of work. Finally she decided to take care of the problem herself without saying anything to the IT security team. After the ransom was paid, the files were restored and a few days later she forgot about the incident.

But unknown to her, the malware was still on the computer. She didn't know that paying the ransom didn't mean the system was clean, even if access to data was restored. Eventually, a significant amount of corporate data in the shared folders became encrypted and the organization itself was held to ransom, bringing to light the whole incident. "

On-time detection is also key to the successful investigation, and forensic analysis, of a targeted attack. Relying solely on employees' vigilance and their ability to report incidents when they happen is not enough, as the risks concerning both human factors and attack sophistication are doubling. It is therefore recommended that businesses use dedicated solutions and technologies that automate system monitoring and reduce the chances of error or irresponsibility.

The 'hide and seek' problem seems to be most challenging for larger companies, with 45% of enterprises (over 1000 staff) experiencing employees hiding cybersecurity incidents, compared to only 29% for VSBs (with under 49 members of staff).



Source: IT Security Risks Survey 2017, global data

The problem of hiding incidents, however, should be communicated not only to employees, but also to the entire business - namely top management and HR departments. If employees are hiding incidents, there must be a reason why. In some cases, companies introduce strict, but unclear rules and impose extra responsibility on employees, warning them not to do this or that, or they will be held responsible if something goes wrong. Such policies only foster fears, and leave employees with just one option — to avoid punishment whatever it takes.

Irresponsible employees – the damage

As well as being irresponsible by hiding incidents when they happen, employee irresponsibility can also have a hard-hitting impact on a firm's data and system integrity when it's linked to a security incident.

For example, 46% have confirmed that those incidents have resulted in their business's data being leaked or exposed because of employee actions. In addition, over one in four (28%) have lost highly sensitive or confidential customer/employee information as a result of irresponsible employees, while 25% have lost payment information. All of these implications, of course, have the potential to have a far-reaching and damaging impact on a business's reputation – both internally and externally.

Below is the story of an advertising firm that lost a real business opportunity after its critical data was exposed, as a result of a minor employee mistake. The story is told by one of Kaspersky Lab's security experts:

A young but ambitious advertising agency finally got a call for a tender from a very big client they had been trying to approach for months. The workload for compiling a successful proposal was huge, the time and resources were limited, and the work group – freelance designers, home-working copywriters, an account manager and an account director – became ridiculously large, also involving several third-party contractors.

To make the process smooth and easy, the agency decided to put a draft of the proposal in Google Docs and only allowed access to the document to people who had the link, namely the group itself. When the proposal was finished, downloaded, and the Google document was closed, the newbie account manager made it available once again — just to secretly show it to a couple of former senior colleagues who could provide them with useful advice before the submission. Only this time, due to his nerves about presenting to the client, the account manager completely forgot about the privacy settings and made the document available to everyone on the web.

So, what happened next? The night before the proposal submission deadline, a more experienced competitive agency decided to do a simple Google Docs extended search (using the combination 'client name + proposal'). They found the document with several nice and creative ideas and, more importantly, the budget estimate for the services. To eliminate the new player in the market, the more established agencies worked together and agreed to lower their prices to make it look like the rookie firm was trying to overcharge. The firm dropped out of the bid and were none the wiser until the disappointed account manager took another look at the proposal in Google Docs to see where they had gone wrong and finally realized – the privacy settings were not enabled!

That's how the advertising firm lost a major new business opportunity because of lack of security awareness and clear security policies in place.

BYOD: employee irresponsibility undermines mobility trends

BYOD concerns vary according to business size

The results of our survey tell us that despite both businesses and employees being well-versed in the trend of bring-your-own-device (BYOD) by now, BYOD is still causing a headache for companies big and small, with 33% of businesses worldwide concerned about BYOD.

For small companies, the concerns generally revolve around employees' BYOD practices, while enterprises are more likely to struggle with security management. For example, almost half (48%) of businesses overall, are worried about employees inappropriately sharing company data via the mobile devices that they bring to work. For small businesses this is a particular concern (57%), perhaps partly due to the fact that these sized businesses tend to adopt BYOD policies more readily to cut costs and appease mobile workforces.

Enterprises, meanwhile, are more likely to find it difficult to manage the security on users' devices. Just over half (51%) said this was a concern for them, compared to two-fifths (42%) of very small businesses.

Device and media exposure: rather a human error than a malicious action

Part of the reason businesses may be concerned with BYOD is due to the fact that BYOD is ultimately dependent on the responsibility of employees, and their ability to treat the business data on their personal devices well.

This process isn't always a smooth one – people lose devices, and devices are stolen. Essentially, the more a device is taken outside of the work environment, the more at risk it (and its data) is.

Our study tells us that over half (54%) of businesses have had data exposed because employees have lost devices.

If employee responsibility is crucial to BYOD working in a company's interests, employee carelessness can be fundamental to the problems experienced with the trend. Indeed, employee carelessness contributed directly to 48% of cybersecurity incidents, accounting for even more incidents than the theft of devices, which only contributed towards a third (37%) of incidents.

So how can we address the employee dilemma?

IT security policies are not enough

It's simply not enough to have an IT security policy in place. A policy, alone, will not protect a business from threats – partly because IT security policies are not always followed by the staff that they are designed for, and partly because they cannot cover every possible risk.

In fact, our research shows that an astounding 44% of companies say that employees do not follow IT security policies properly. What's even more concerning, is that even though two-fifths of businesses have admitted to us that employees do not follow their security policies, businesses are doing little to help solve the problem themselves, with only a quarter (26%) planning to enforce their IT security policies among staff.

In many cases, policies are written in such a difficult way that they simply cannot be effectively absorbed by employees. Instead of communicating risks, dangers and good practices in clear and comprehensive instructions, businesses often give employees multipage documents that everyone signs but very few read – and even less understand.

The right step forward

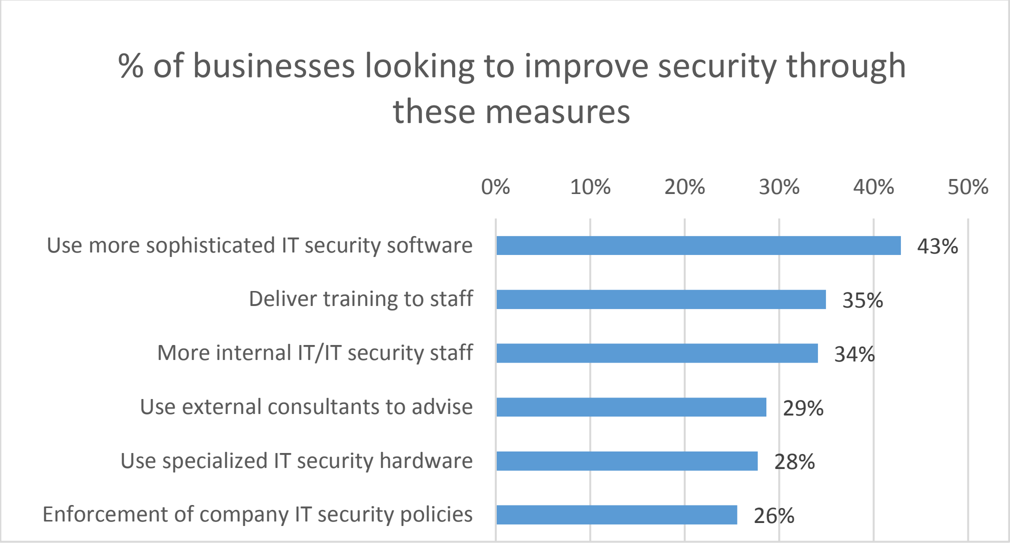
But it's not all doom and gloom. Despite the evident challenges, businesses are trying to solve the issue of the risk from within. Training personnel and bringing more dedicated staff on board to help enforce security policies is a logical answer to the problem of employee carelessness. And it's the answer that multiple businesses across the globe are looking to implement.

As we have already seen, having security policies in place is not enough. The right balance should be struck between policy and engagement, in order to help prevent staff carelessness, or dangers due to uninformed staff.

Staff training is essential in raising awareness among personnel and motivating them to pay attention to cyberthreats and countermeasures — even if they are not part of their specific job responsibilities. Installing updates, ensuring that anti-malware protection is on, and managing personal passwords properly shouldn't always be at the bottom of an employee's to-do list.

To-Do List
• call mom
• Put my lunch in the fridge
• Cancel my Karate class on Tuesday
• Chat with Angie about the party
• Change my password

Employee-focused security measures such as employee engagement and training are among the most popular tactics being used by businesses to safeguard themselves against future cyberthreats.



Source: IT Security Risks Survey 2017, global data

As the chart above shows, delivering training to staff is the second most popular method of defense for businesses – second only to the deployment of more sophisticated software and closely followed by increasing the numbers of internal IT or IT security staff.

At Kaspersky Lab, we know that the best way of protecting a business from cyberthreats is a combination of the right tools and practices. In addition to awareness training for staff, protection should include security solutions that make the corporate network more visible and manageable for IT security teams.

Most of the threats related to unaware or careless employees, including spam, phishing and ransomware, can be addressed with endpoint security solutions. There are tailored products that can cover particular needs of SMB and Enterprise-level companies in terms of functionality, pre-configured protection or advanced security settings.

Overall, while there is evidently much more work to do before businesses are secure from the actions of their own employees, it is nevertheless refreshing to see that many businesses are recognizing this, and starting to address the threat from within, with additional training, solutions and human resources.

Conclusion

Our research has shown that businesses are at a very real danger of threat from within. They are aware of how easy it is for employee or human error to impact a company's security, with careless or uninformed staff being the second most likely cause of a serious security breach, and they are searching for a way to mitigate risk.

Staff can, according to this report, become attack vectors in many forms: they may be careless, they may be uninformed, or their actions might be malicious. Mobility trends mean that careless or uninformed staff may become more likely to make mistakes, and threats such as phishing and social engineering also put businesses more at risk from staff that do not know how to spot the difference between legitimate and malicious activity. When they have caused a cybersecurity incident (or been one of the factors behind an incident), staff, moreover, may be likely to hide what has happened, leaving some breaches undiscovered for longer and businesses even more at risk.

Acting now, to prevent employee-related threats, has never been more important.

While having security policies in place is vital, businesses also need to recognize that policies cannot cover all the risks. Moreover, staff don't always follow their policies to the letter. There is a clear need for solutions that provide more visibility and centralized security management of corporate networks, combined with training, so that employees can become more aware of the impact of their actions. It is only through educating staff about the importance of working safely, that businesses can help to mitigate the risk of this particular attack vector, and safeguard what is most important to them – their data.

For more info contact us at: intelreports@kaspersky.com
(Kaspersky Security Intelligence Service)

Securelist, the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy