Bitdefender®

# Hacked Off!

2019

# Introduction

## Introducing Bitdefender Hacked Off! A comprehensive study into the cybersecurity attitudes of infosecurity professionals around the world

"From organisational weaknesses to infosec professionals' pressure points and what they're doing to combat them, Hacked Off! aims to shine a light on the current state of play of the global cybersecurity landscape by focusing on three core areas:

### Weak spots

Exploring individuals' perception of risk and the top internal and external threats facing organisations

### Stress

Analysing the most significant stress factors for infosec professionals, as well as the training and support available to them

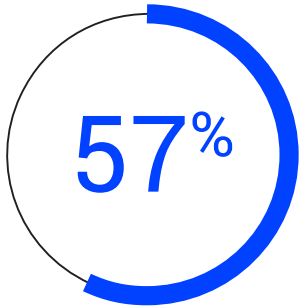
### Strategy

Hearing directly from cybersecurity professionals about their current infosecurity strategies and plans to safeguard their organisations

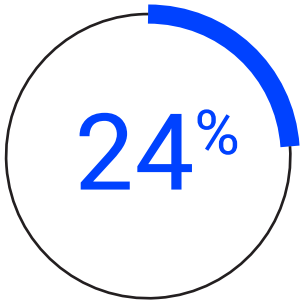
"This Bitdefender survey of more than 6,000 infosec professionals in large organisations across the US, EMEA and APAC shows that while many rate their cybersecurity as 'good', a continued lack of budget, talent and training means that there is still significant scope for improvement. A large portion of them believe that the best way of defending against advanced attacks is to provide training & support. This is proved by the fact that organisations which are placing more emphasis on training are better at detecting attacks quickly, and more efficient at isolating them. Ultimately, cybersecurity has improved over the last 36 months, but IT workers are still facing a great deal of stress and risk. This means that getting the right strategies and solutions in place is imperative. In fact, it will ensure the trend of stress and risk doesn't stretch into future years."

**Bogdan Botezatu, Director or Threat Research at Bitdefender**

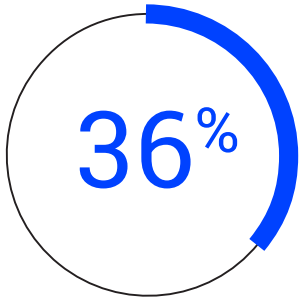
# Introduction




of companies **have experienced** a breach in either 2017, 2018, or 2019




of companies have **already suffered** a data breach halfway through 2019




of companies who haven't suffered a cyber attack, believe that it is likely that they are **currently facing one** without knowing about it

# Introduction

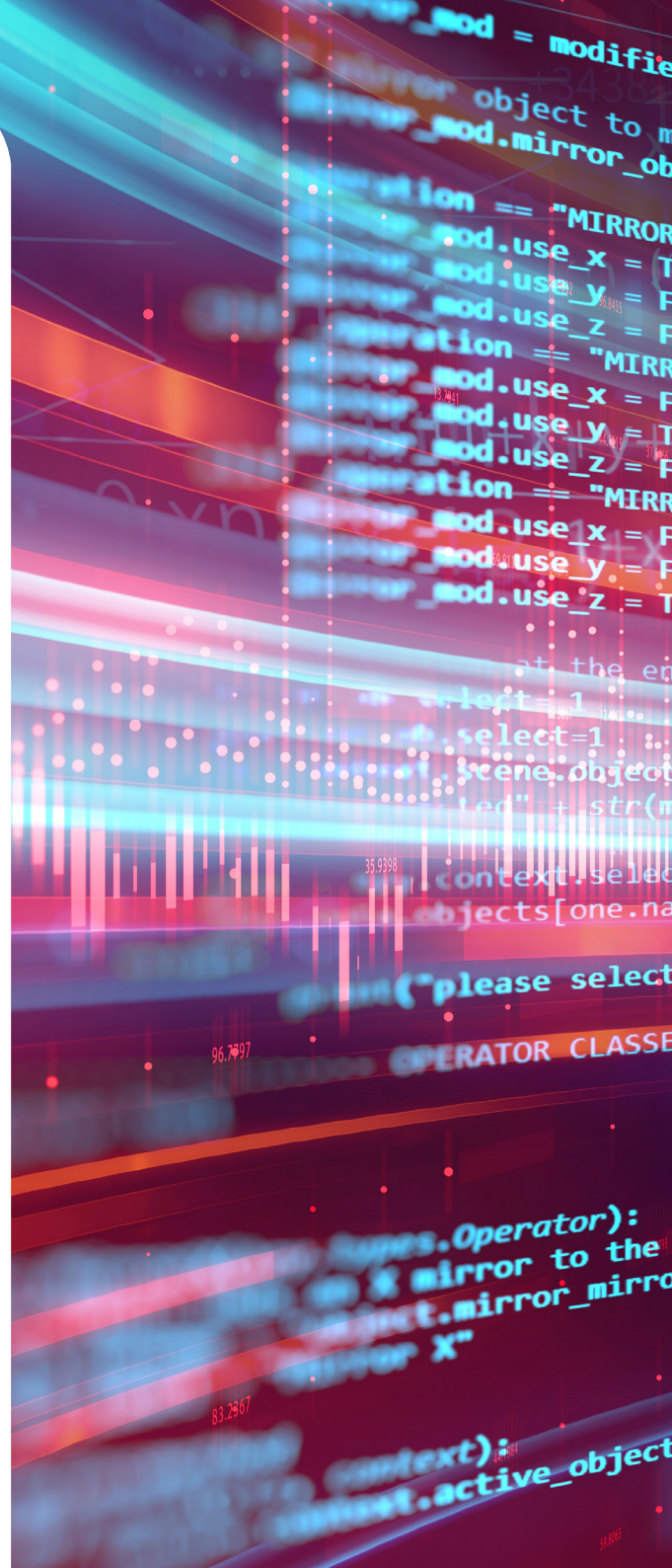
“In the last 12 months, cybersecurity professionals have had to step up their game. As the threat landscape has grown more complex, more comprehensive infosec strategies and solutions have had to be employed to protect business continuity. However, there are still gaps.

“From squeezed budgets and inadequate training to a lack of talent and resourcing, the door has been left ajar for determined cybercriminals to exploit all but the savviest of organisations. Additionally, with the media’s continual focus on cybersecurity failures, organisations which are left exposed to threats could very well find themselves with all the wrong sorts of publicity. It’s no wonder infosec professionals are feeling hacked off!

“CISOs and infosec professionals are, however, acknowledging the steps needed to better protect their businesses improve. For example, a lack of time is a huge factor and a massive weak spot for many organisations. The fact that many infosec professionals are aware that this needs to improve is the first step to fixing the problem. Additionally, the tools available and the understanding of cybersecurity far exceeds previous years, but there is still a risk of becoming complacent. Everyone, from the CISO to the IT professional has to understand that cybersecurity is a constant, ongoing process. Modern business requirements and an advancing threatscape now require that strategies are regularly evaluated and improved upon.

“So what does all this mean for cybersecurity in 2019? Especially for those whose organisations’ have already been subject to attack, it may mean many more sleepless nights are ahead. However, it’s not to say that things can’t get better.”

**Bogdan Botezatu, Director or Threat Research at Bitdefender”**




## Assessing the threatscape:

# Weak Spots

No organisation is impervious to a data breach, but by understanding how both cybersecurity professionals and IT departments view risk, some clear weak spots start to emerge — both on an organisational and individual level. Highlighting areas for improvement can only happen through increasing visibility.

# Weak spots

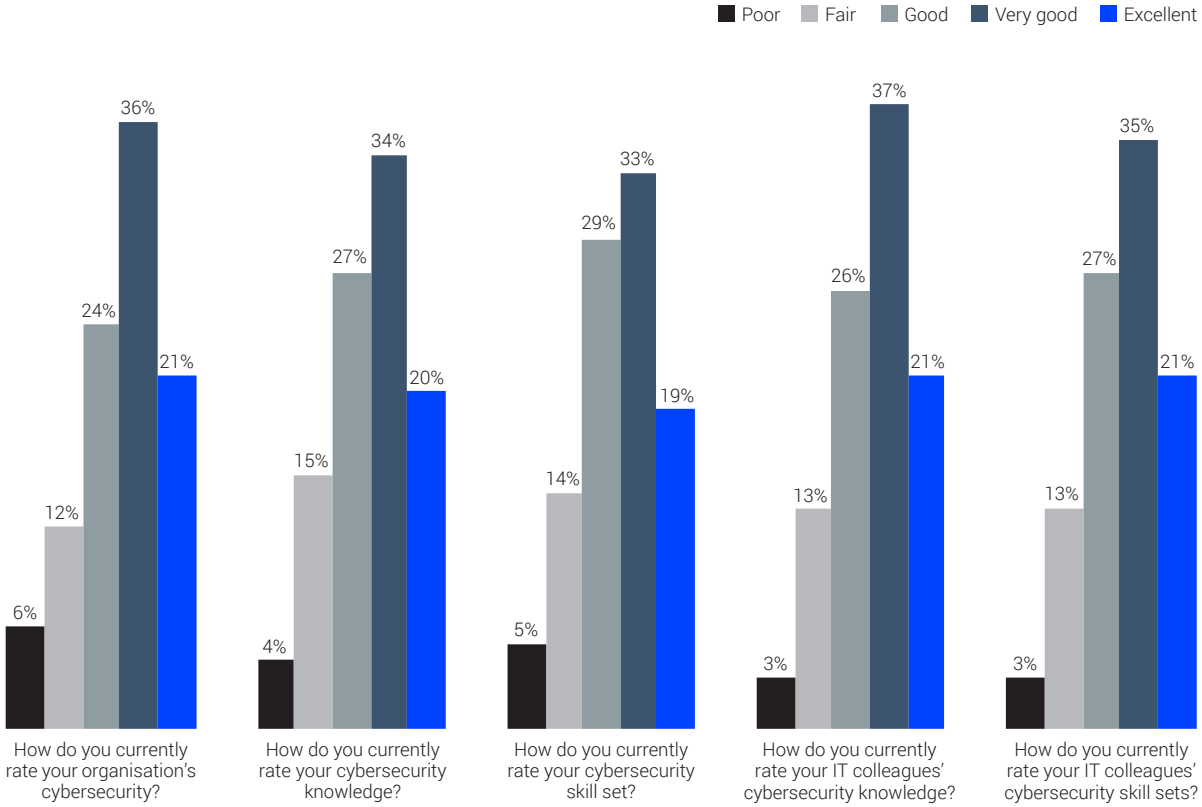
## Skills and the state of security

Infosec professionals' view of their organisational cybersecurity is, on the whole, fair or good. But, there is room for improvement.

57% of infosec professionals rate their organisations' cybersecurity either very good or excellent. Another 24% believe that it is good. This shows that the majority of IT workers are reasonably confident in their organisation's cybersecurity position.

However, just shy of one in five infosec professionals (19%) say cybersecurity skills are excellent, and 21% say they would rate their IT colleagues skills as excellent. Overall, cybersecurity knowledge seems to be high, but with an increasingly complex threat landscape, skills improvement is an area in need of investment.

**How do you currently rate your organisation's…?**



# Weak spots

## It's a minefield out there

### What are the biggest infosec threats to organisations in 2019?

Out of the possible threats to an organisation, 36% of IT workers think phishing or whaling attacks pose the biggest threat. Understandable, given the fact that phishing is often used to break into corporate networks, paving the way for more damaging attacks i.e. Carbanak.

However, across Europe, this differs considerably; for example, 43% of IT workers in Germany see phishing / whaling the biggest threat, compared to 33% in Spain.

Comparing this to 2018: the biggest threat was ransomware (20.4%) and phishing / whaling was only 10.8%. This is evidence of an ever-evolving threat landscape and highlights why organisations have to keep on their toes.

**Which type of cyber attack / cyber risk, in your opinion, poses the biggest threat(s) to your organisation in 2019?**

36%
Phishing / whaling attack

29%
Trojans

28%
Ransomware

28%
Legal and compliance risks

24%
Unpatched software

24%
DDoS attack

22%
Social media threats

20%
APTs and cyber espionage

0%
Other

4%
Don't know

# Weak spots

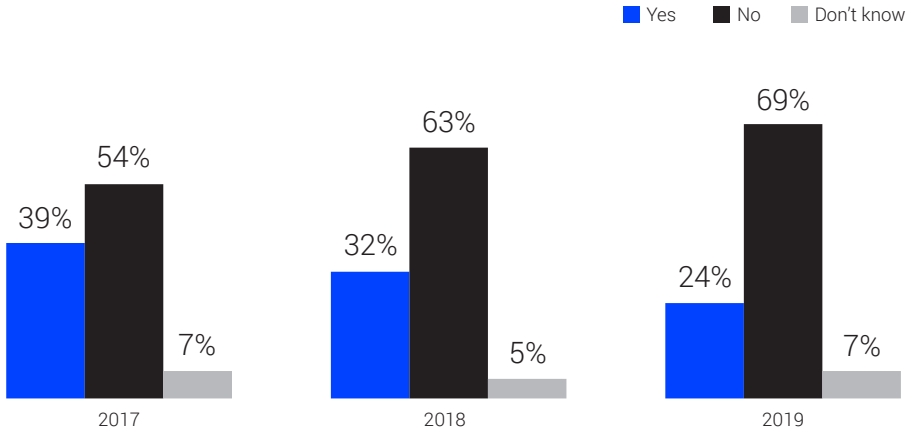
## A new era for breaches

### Organisations are still experiencing breaches, but has the threat improved over time?

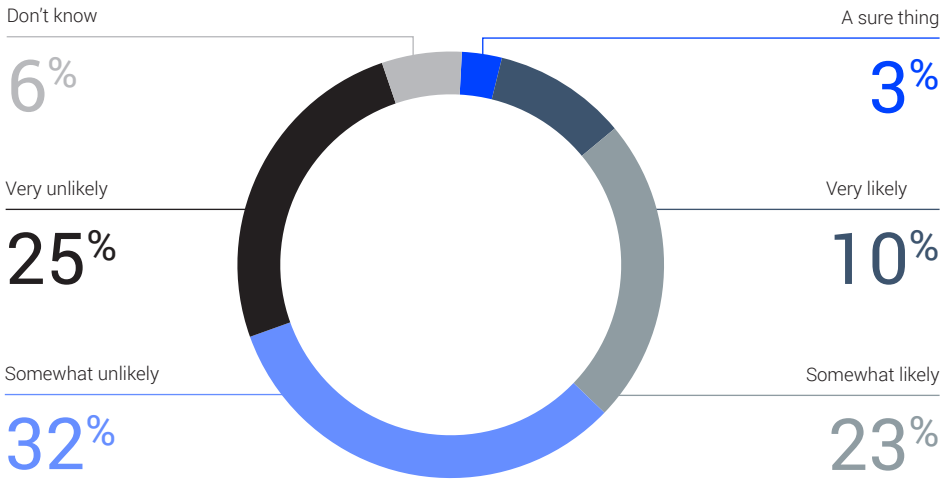
Over the past three years, the number of companies suffering from data breaches has decreased, which is positive.

However, 36% of infosec professionals think their companies are likely facing a cyber attack without knowing about it. This raises questions over whether breaches have declined, or whether organisations are finding it more difficult to identify that data has even been exfiltrated from their organisation.

**Did your company suffer a breach in…?**




**How likely it is that you are currently facing a cyber attack without knowing about it?**




### Geographical differences

In 2017, 50% of companies in Spain suffered from a data breach compared to only 39% globally. In 2019, 24% of companies globally suffered from a data breach, compared to just 13% in Italy.

Consistently, companies in Italy scored the highest for reporting that they had not suffered a data breach. Is this a cultural reason, or something more?

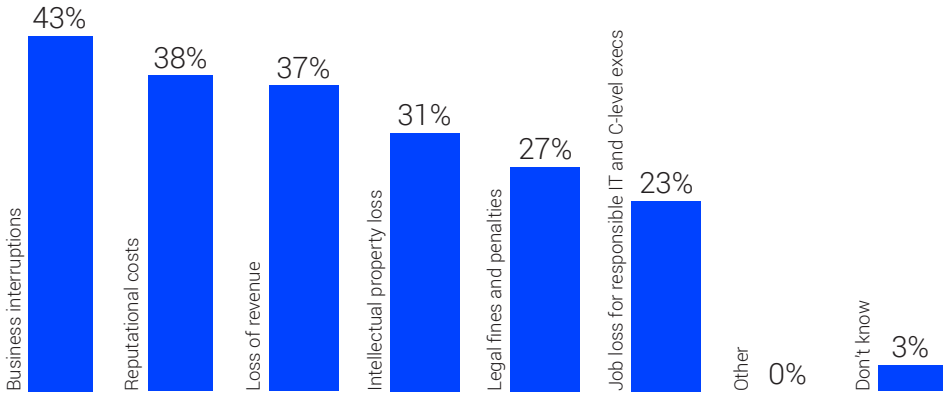
# Weak spots

## Data breaches: consequences and outcomes

### We know that breaches are happening, but what does it mean for an organisation?

Business interruption is seen as the main consequence (43%) amongst infosec professionals of being unaware of a currently ongoing breach. Understandably, this can have a detrimental impact on an organisation, resulting in loss of customers and / or revenue.

**What would be the main consequences for your company of being unaware of a currently ongoing breach?**




Whatsmore, only 27% of respondents would see legal fines and penalties as the main consequence of their company being unaware of a current, ongoing breach. This is surprising, given the recent high-profile GDPR fines. Does this suggest that the current penalties aren't working in terms of driving organisations to improve their security posture?

### Industry interruptions

Over half (52%) in manufacturing see business interruptions as the main consequence

Compared to retail, where the main consequence is believed to be loss of revenue (51%).

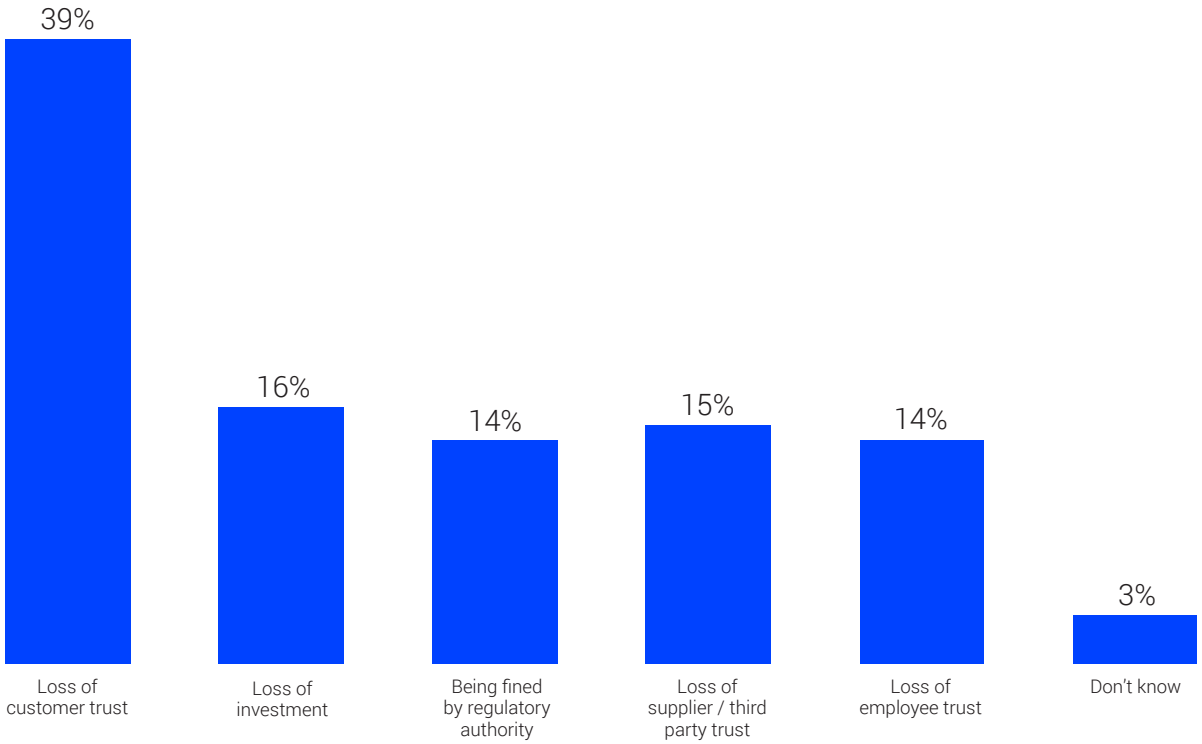
# Weak spots

## Data breaches: consequences and outcomes

### We know that breaches are happening, but what does it mean for an organisation?

Looking ahead to long-term outcomes of a large scale breach, IT C-suiters still cite a loss of customer trust to be their biggest concern (39%), should their organisation be breached tomorrow. It was also its top concern last year (42%).

**What would you be most concerned about should a data breach happen at your organisation tomorrow? (IT C-suite)**



# Weak spots

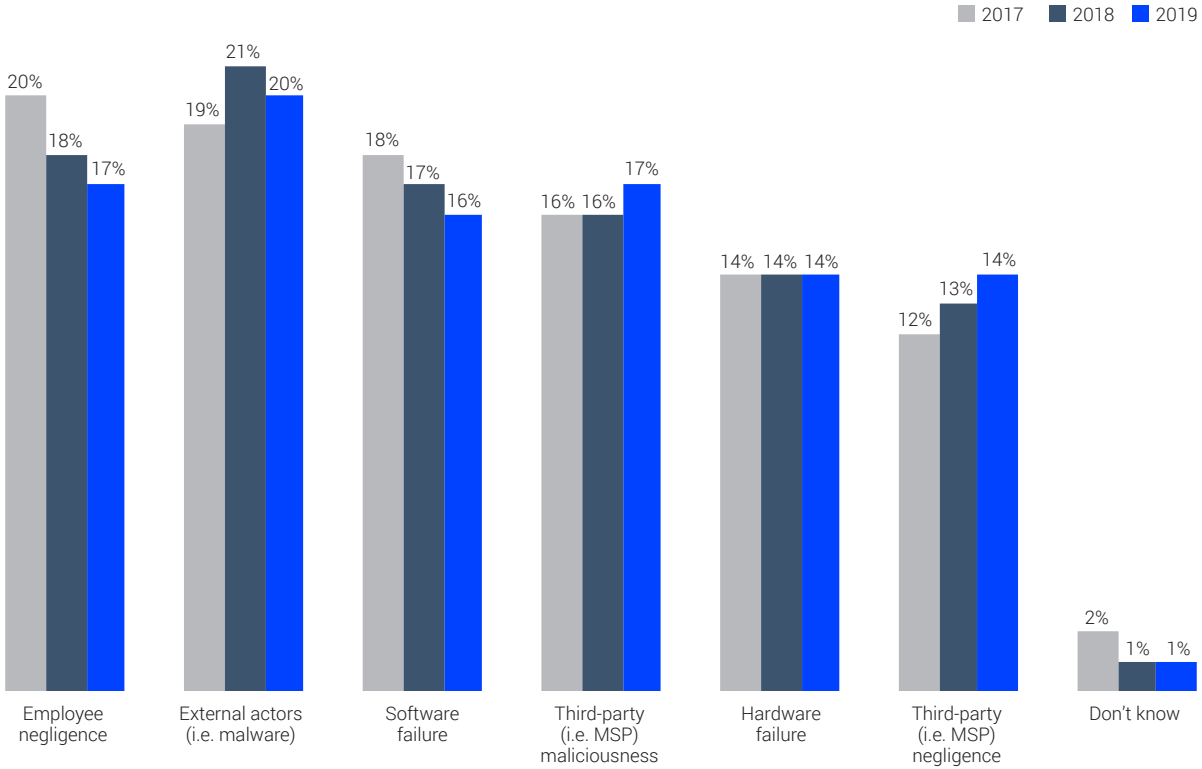
## The cure and the cause

The reasons behind security breaches have changed over the past three years, but some key culprits remain.

Over the last three years nearly two fifths of all data breaches were due to either external actors (e.g. malware) or employee negligence. However, employee negligence as a cause of a company's data breach has declined over the last three years, suggesting that there is now a better understanding of correct infosecurity practices.

Software failure has, however, remained relatively consistent throughout the last three years as the cause of a data breach. This is an interesting point as despite software becoming more advanced, it is not necessarily risk-free.

**How was your company breached in…?**



# Weak spots

## Playing by the rules

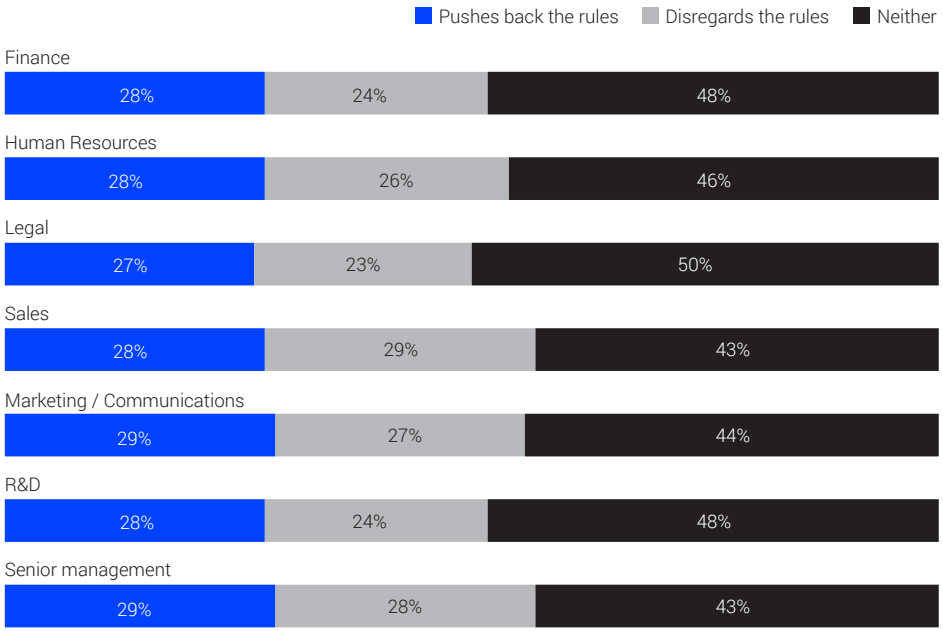
While push back on infosecurity rules isn't entirely unexpected, it's concerning that some roles and departments seem to disregard them altogether.

The majority of infosec professionals believe their financial department is most at risk from a data breach.

**Which department / area in your organisation would you say is most at risk of a data breach?**


While there aren't great differences in regards to departments which push back / disregard organisational cybersecurity policy, it does somewhat correlate with the departments that are deemed as most 'at risk'. Legal pushes back the least, while senior management the most.

**Which department in your company pushes back / disregards the rules the most in regards to organisational cybersecurity policy?**



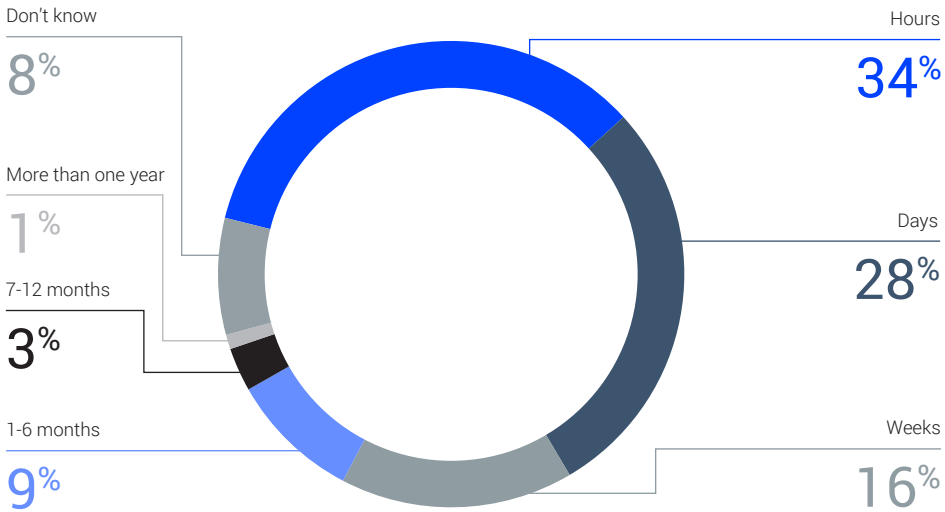
# Weak spots

## Time is of the essence

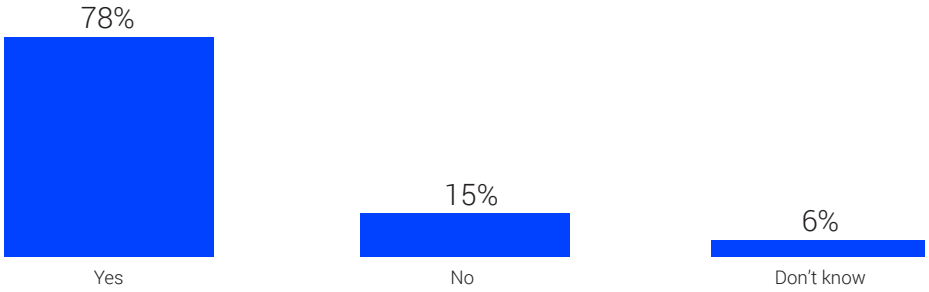
Most cybersecurity professionals claim to spot advanced cyber attacks quickly, but why is it important to detect at speed?

The majority of infosec professionals (78%) believe that reaction time is the key differentiator for mitigating cyber attacks

**How long would it take you to detect an advanced cyber attack, i.e. an attack that utilised a zero-day exploit**




**Is reaction time a key differentiator in mitigating cyber attacks?**




Given the emphasis on the importance of time, the majority of companies claim they could detect an advanced cyber attack within hours. But if reaction times are this good, why are threats still going unidentified?

### In agreement, regardless of role

82% of security directors see reaction time as the key differentiator in mitigating cyber attacks

The majority of day-to-day IT workers (78%) believe that reaction time is the key differentiator for mitigating cyber attacks, with 81% arguing that this is so they can identify the source of the attack, isolate it and stop it from spreading .

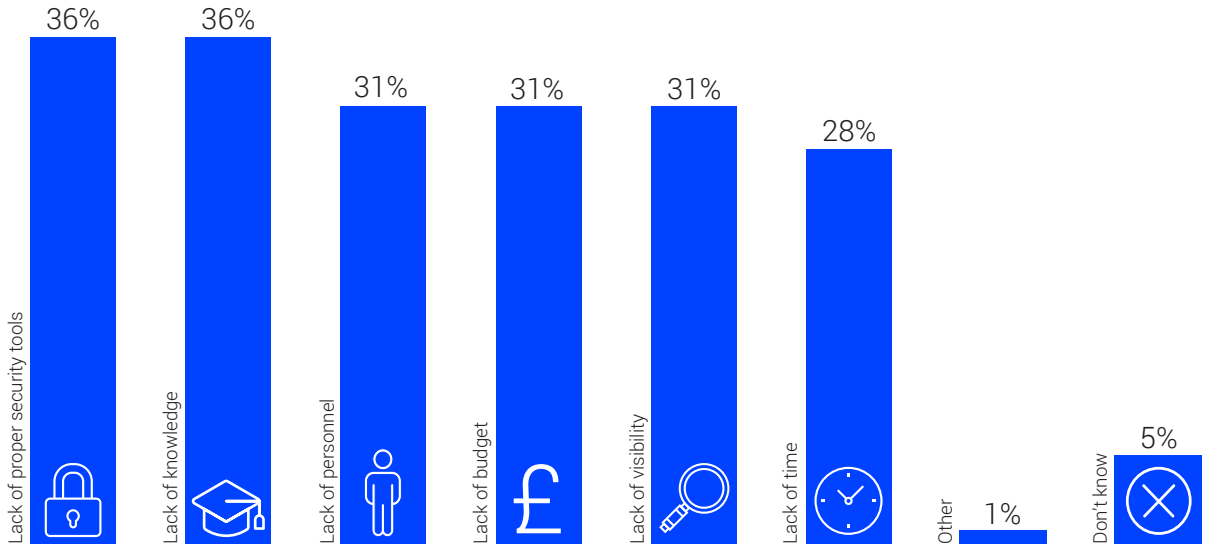
# Weak spots

## Breaking down barriers

Despite the majority of infosec professionals having confidence in their organisations' cybersecurity, there are still obstacles to overcome.

According to 72% of infosec professionals, a lack of proper security tools and knowledge are considered the main obstacles that prevent rapid incident detection and response. In fact, 42% of the infosec C-level think a lack of proper security tools within their organisations are the main obstacle preventing rapid incident detection and response.

**What are the main obstacles that prevent rapid incident detection and response?**



# Weak spots

The threat landscape evolves rapidly. External threats that were commonplace three years ago have shifted, but that's the nature of the beast when working within information security. The good news is that breaches have slightly fallen since 2017, and, for the most part, infosec professionals are confident in their organisations' cybersecurity capabilities.

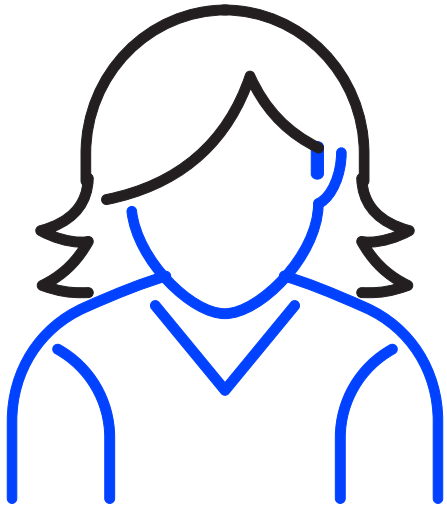
However, confidence isn't breeding complacency. There are still concerns that budget and personnel are lacking when it comes to meeting some current and future challenges.

Additionally, not all employees are playing ball across the business when it comes to following the rules. If corners are going to be cut in the name of getting the job done quickly, then robust solutions need to be in place to catch any resultant mistakes.

With all this in mind, it's understandable that infosec professionals are feeling stressed, but just how is this affecting their roles?

**Liviu Arsene, Global Cybersecurity Researcher at Bitdefender**

Bitdefender



## Influencing security decisions:

# Stress

Organisational weak spots and infosecurity stressors go hand in hand. From employees lacking training to basic cyber negligence, uncovering what keeps infosec professionals up at night is the first step towards implementing strategies that can help individuals in their roles, and their organisations more widely.

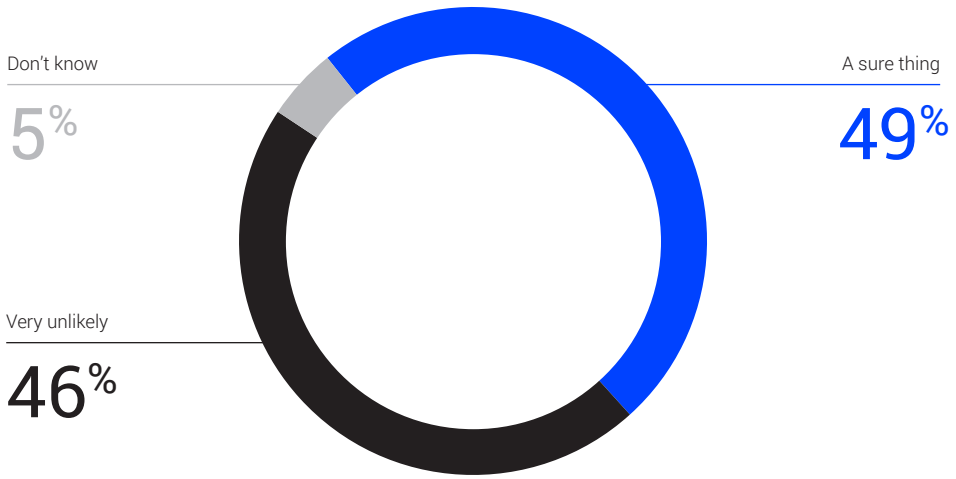
# Stress

## What keeps infosec professionals up at night?

### Stress is common in most jobs, but what is the number one stressor for cybersecurity professionals?

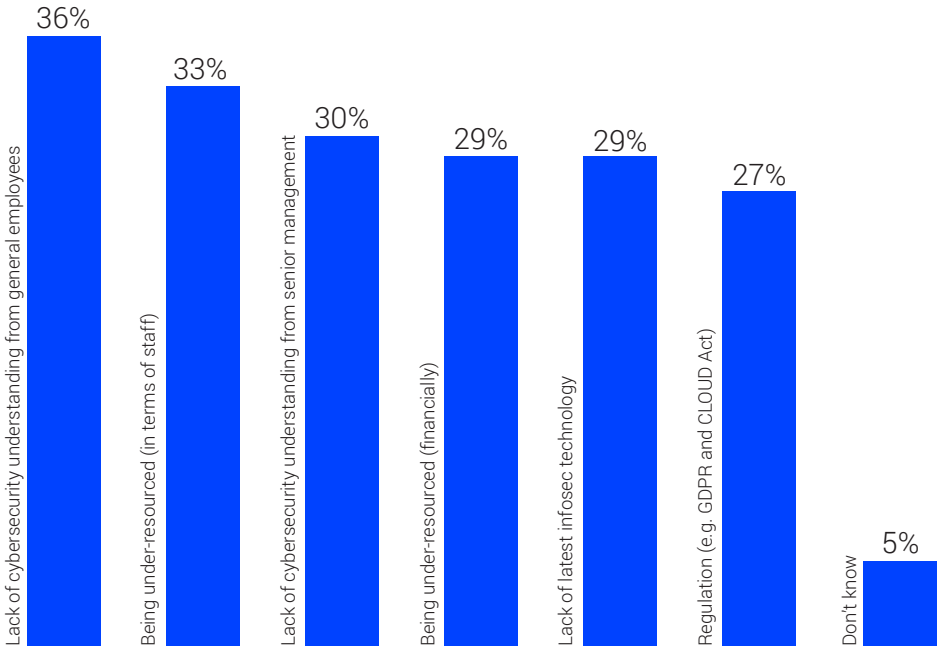
While still a pressured role, the IT C-suite is getting more sleep than it used to. Just under half (49%) are losing sleep worrying about their organisational cybersecurity, compared to 58% just 18 months ago.

**Have you ever been kept awake at night worrying about your organisation's cybersecurity? (IT C-suite)**




A lack of cybersecurity understanding from day-to-day knowledge workers is IT professionals' number one stressor (36%) in regards to their role, followed by being under-resourced in terms of staffing (33%) and a lack of cybersecurity understanding from senior management (30%).

**What causes you the most stress in your role in regards to cybersecurity?**



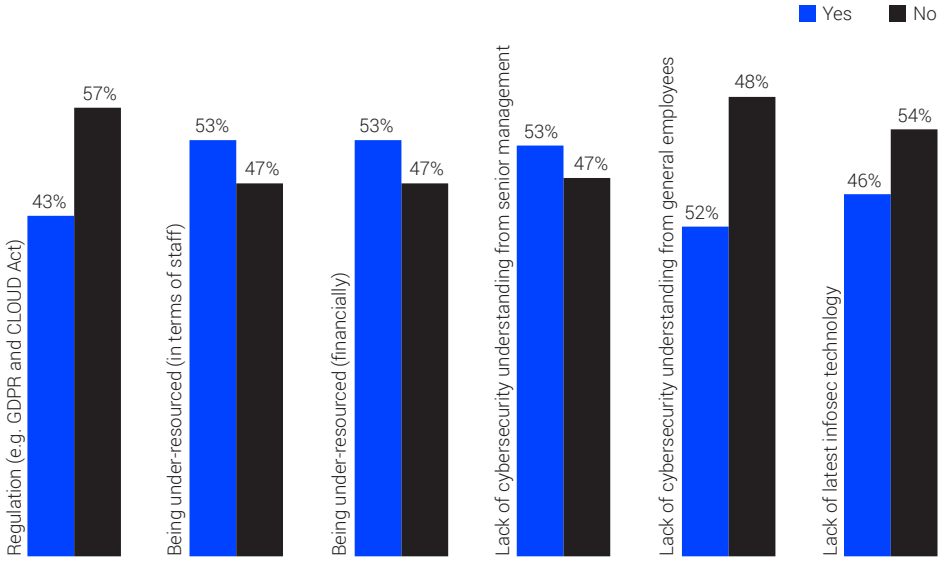
# Stress

## Understaffed and under-resourced

### The impact of lack of resource on staff, and wider organisational risk, is impossible to ignore.

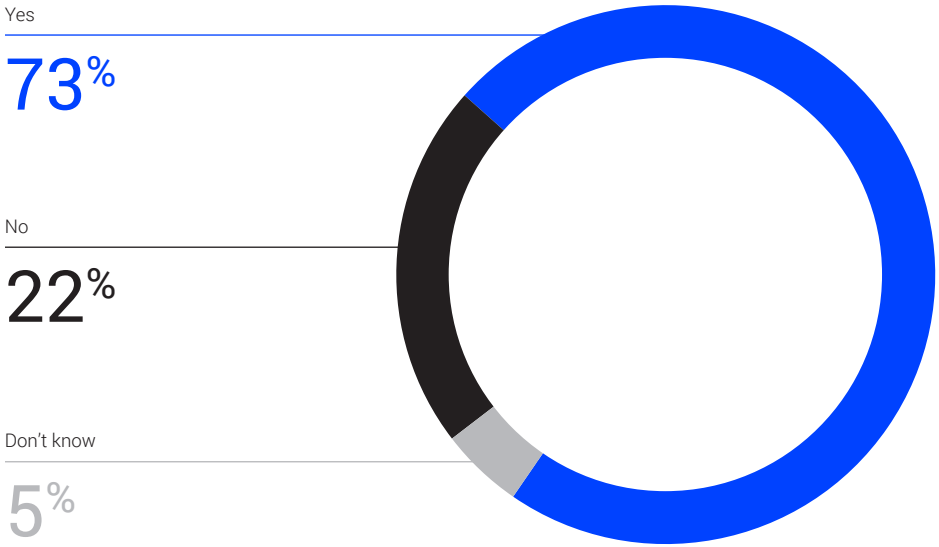
Over half (53%) of security professionals have considered leaving their current role due to being under-resourced both financially and in terms of staffing.

**Have any of the following caused you to ever contemplate leaving your job?**




Unsurprisingly, under-resourcing and cyber attacks go hand in hand, with nearly three quarters (73%) of security professionals saying their organisation is at risk of an attack due to resourcing issues.

**Do you think your organisation is more at risk of a cyber attack as a result of being under-resourced?**



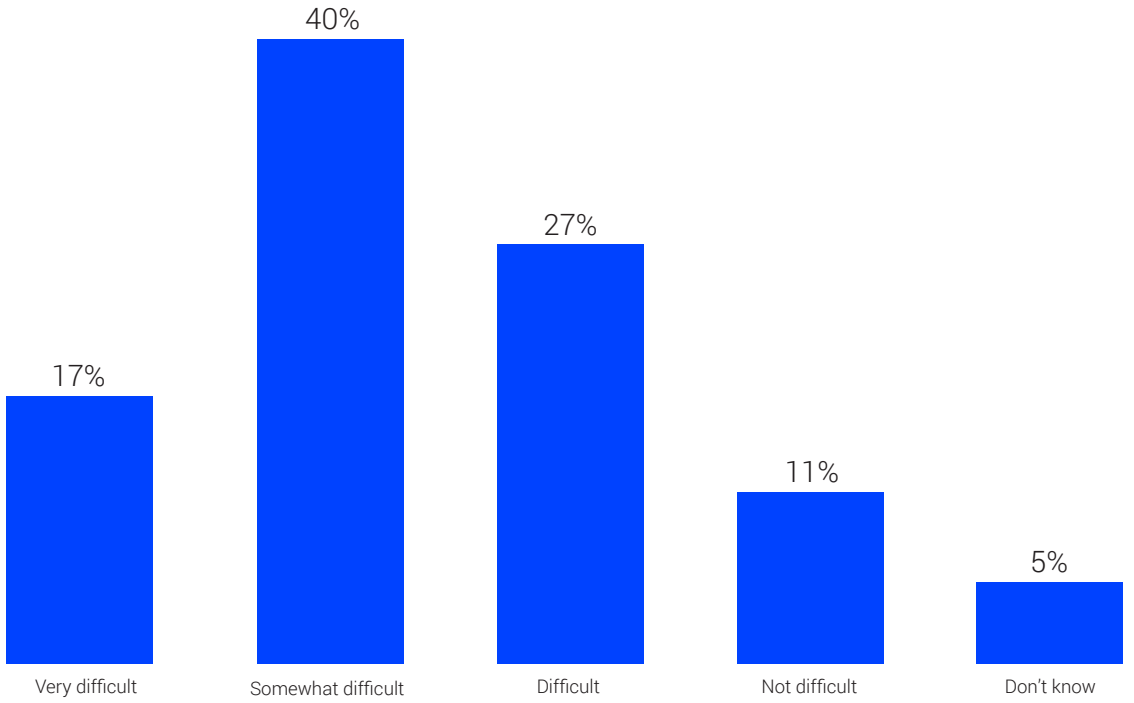
# Stress

## Understaffed and under-resourced

The impact of lack of resource on staff, and wider organisational risk, is impossible to ignore.

Infosec professionals are struggling when it comes to managing their detection and response capabilities in terms of staffing and time consumption, with a massive 84% finding it difficult to some degree.

**How difficult is managing detection and response capabilities in terms of staffing and time consumption?**



# Stress

## History repeating itself

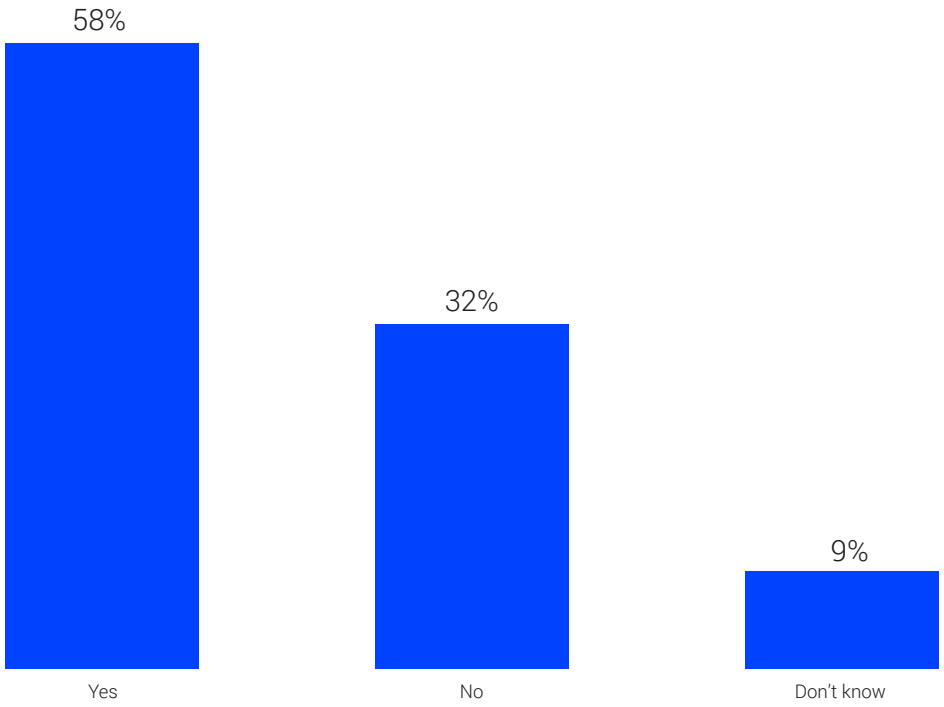
As one of the most well-known breaches of recent years, have organisations learnt their lessons to prepare for another global security crisis on the scale of WannaCry?

Industry isn't blind to large scale cybersecurity threats, but it's clear that some businesses still haven't learnt their lesson with 32% of infosec professionals feeling they couldn't cope with another global cyber attack such as GoldenEye or WannaCry.

### Geographical differences

This again differs considerably based on the country. For example, 73% of IT professionals in Spain would be worried about their companies' infosec readiness if faced with a global cyber attack, compared to 51% in Germany. Misplaced confidence, or better preparation?

**If another global cyber attack similar to the scale of WannaCry struck, would you be worried about your organisation's infosec readiness?**



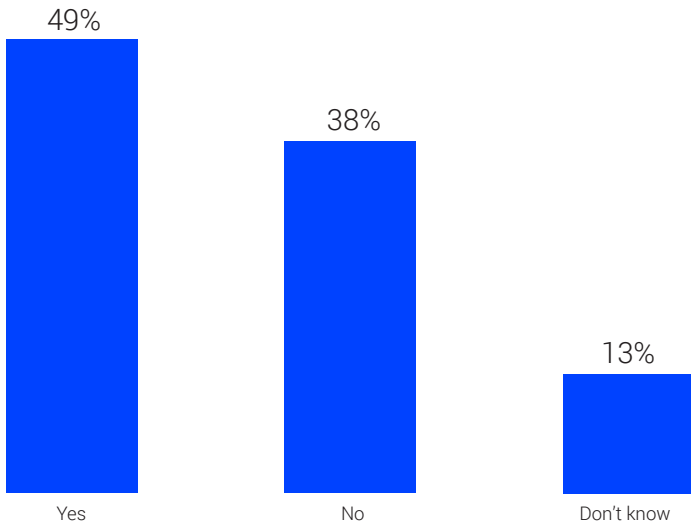
# Stress

## Getting over alert fatigue

IT teams are getting fed up with the number of alerts from infosec solutions, but becoming desensitised carries its own risks...

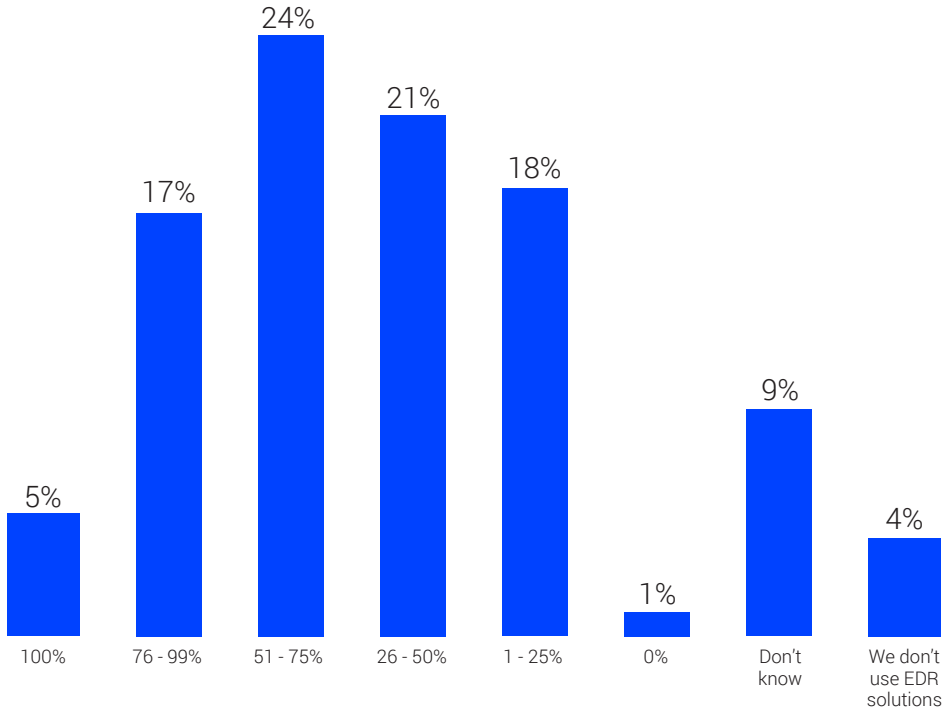
Just under half (49%) of IT teams are getting fed up with the significant amount of alerts from their infosec solutions.

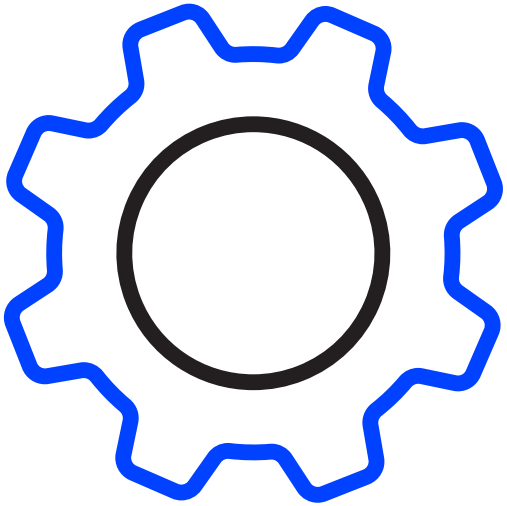
**Does your IT team experience both alert and agent fatigue?**




Of the respondents surveyed, a significant 63% found that up to 75% of their endpoint detection and response (EDR) alerts were false alarms. While being adequately prepared in the event of a breach is important, the sheer number of alerts runs a very real risk of desensitising infosec professionals.

**Of all the endpoint detection and response (EDR) alerts your security team handles, how many are false alarms?**





## Safeguarding organisations:

# Strategy

With areas for improvement highlighted, infosec professionals can start to assess whether their current cybersecurity strategy is fit for purpose. But having a good strategy isn't enough by itself — it'll need to be put into practice, and be backed up by a combination of the right technology, the right talent and a thorough understanding of the risks facing the organisation.

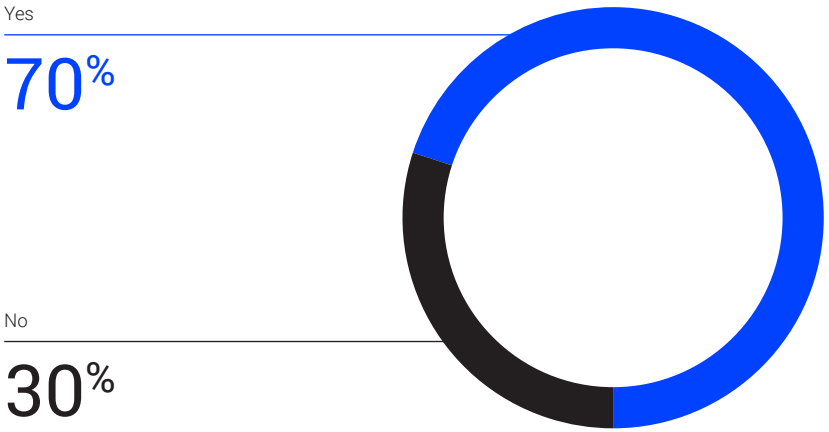
# Strategy

## Teamwork makes the dream work

### Having the right technology to protect against threats is one thing, but what about building an effective team?

70% of organisations have a SOC (a team of IT security specialists that deals with security issues — 24/7 proactive monitoring and threat hunting — on an organisational and technical level). This is positive because having a dedicated team means there is less room for oversight or error when it comes to cybersecurity.

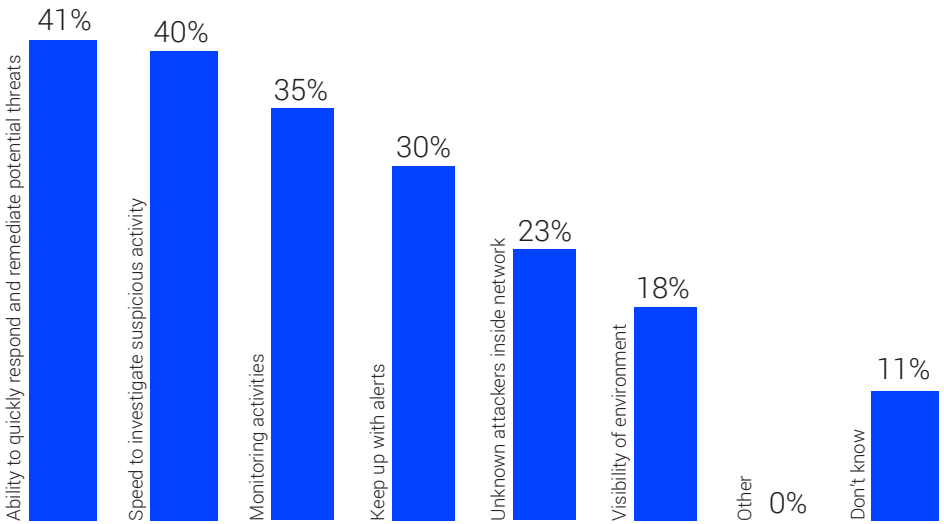
**Do you have a security operations centre (SOC)?**




However, this is easier for businesses with more resources, as three quarters (79%) of large organisations have a SOC compared to just 60% of small organisations.

Three in ten organisations (30%) don't have a SOC, and of these organisations, 81% regard the ability to respond quickly and remediate potential threats as well as the speed to investigate suspicious activity, as the biggest challenges of not having one. This is telling in light of the above findings that the reaction time and speed are the key differentiators for mitigating an attack.

**If you don't have a SOC, what challenges does this create?**

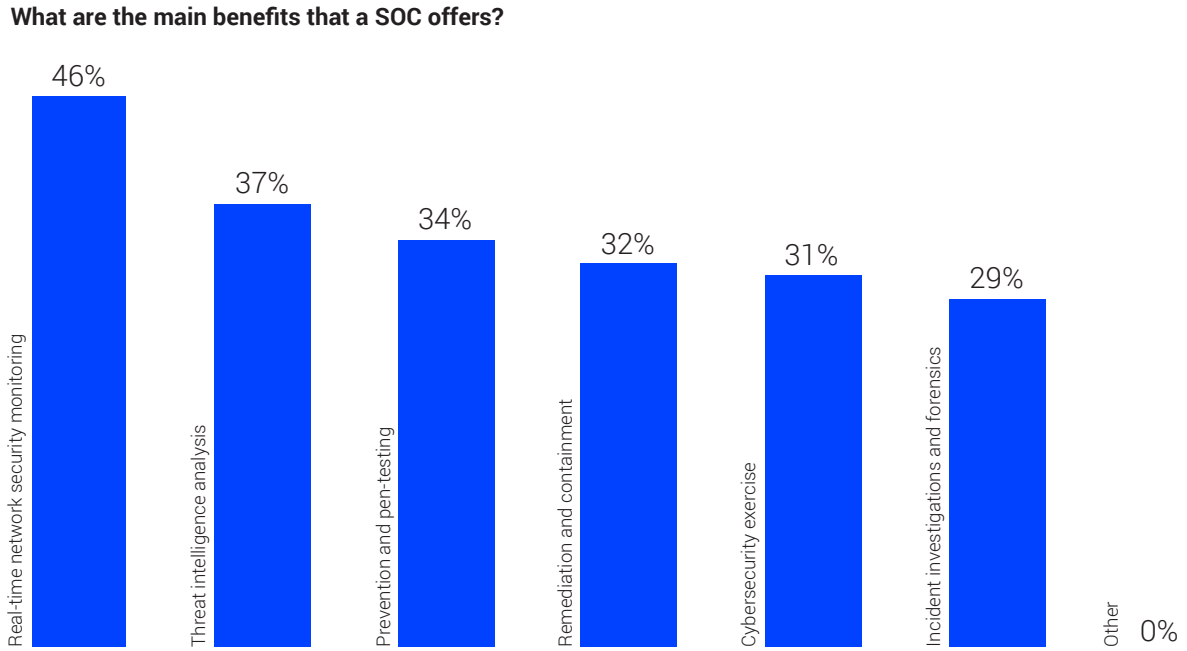


# Strategy

## Teamwork makes the dream work

Having the right technology to protect against threats is one thing, but what about building an effective team?

Just under half (46%) of infosec professionals perceive the main benefit of a SOC being its ability to monitor networks in real-time for security vulnerabilities.



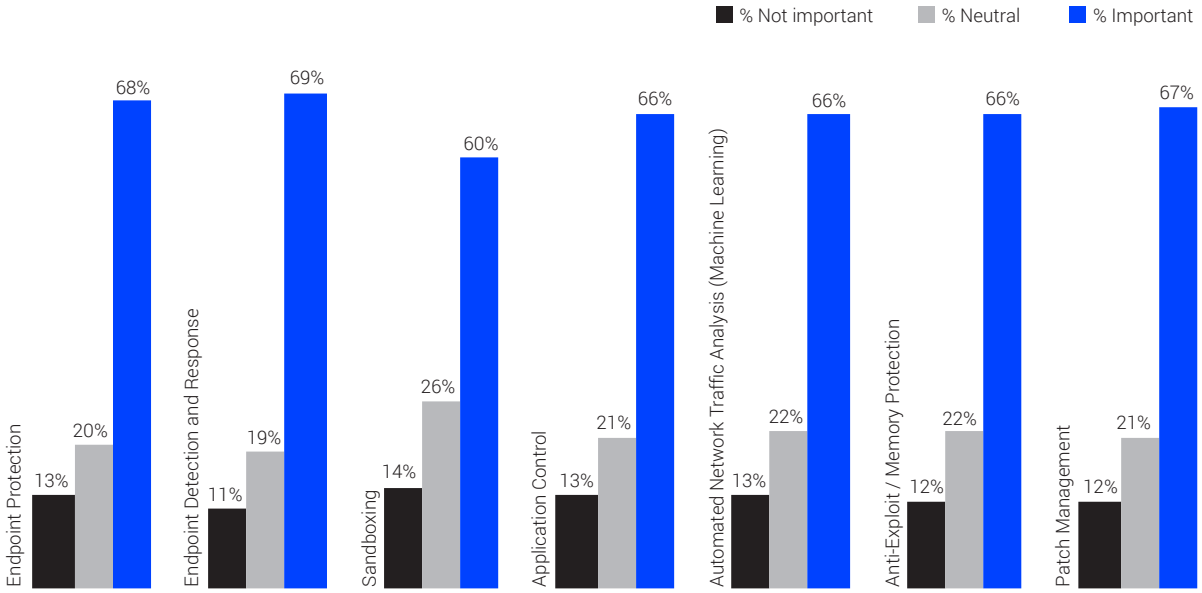
# Strategy

## The faster the reaction, the better the result

### Speed makes a difference, but how does it differ across an organisation's tech stack?

Speed is rated as being important across the security stack by roughly two-thirds of infosec professionals. The consensus being the faster you can react, the faster you can isolate and remediate against cyber threats.

**How important is speed, for example, the ability to rapidly identify/ isolate threats, in each of the following elements of your security stack?**



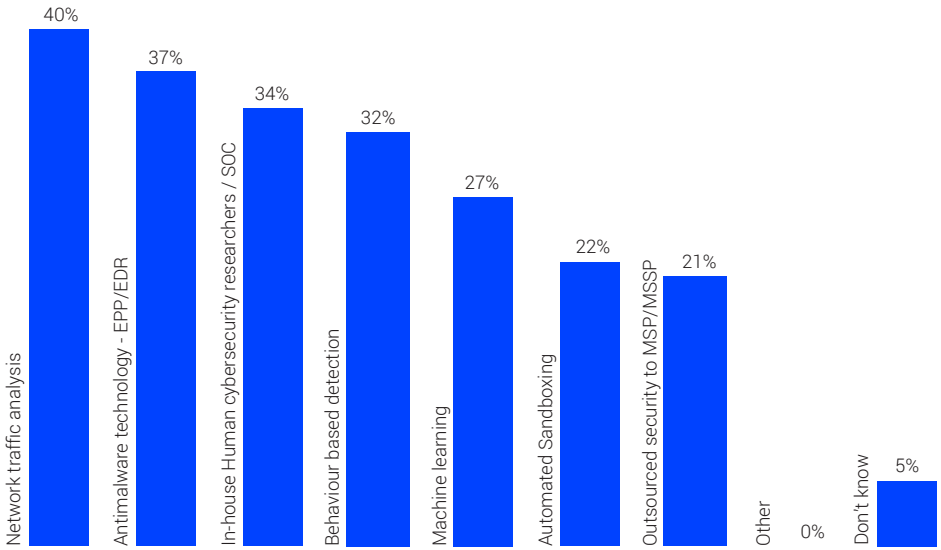
# Strategy

## Creating a smart detection strategy

### What are infosecurity workers using to stay protected?

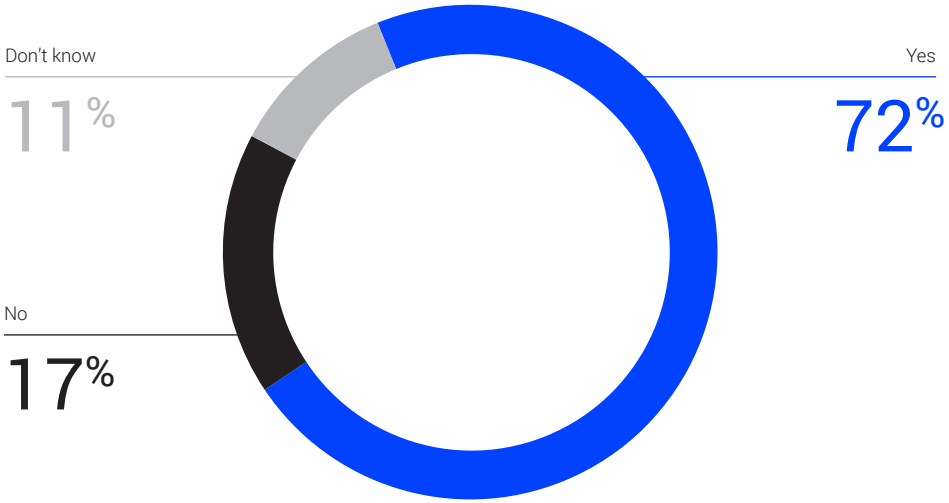
Network traffic analysis and antimalware technology top the list at 40% and 37% respectively in regards to the technologies that cybersecurity professionals cite as being the most effective at detecting cyber threats.

**Which do you think is most effective in detecting cyber threats?**




The overwhelming consensus from infosec professionals is that EDR tools will be essential to help prevent future attacks (71% agree).

**Do you think forensic capabilities and visibility tools (EDR) help prevent future attacks?**



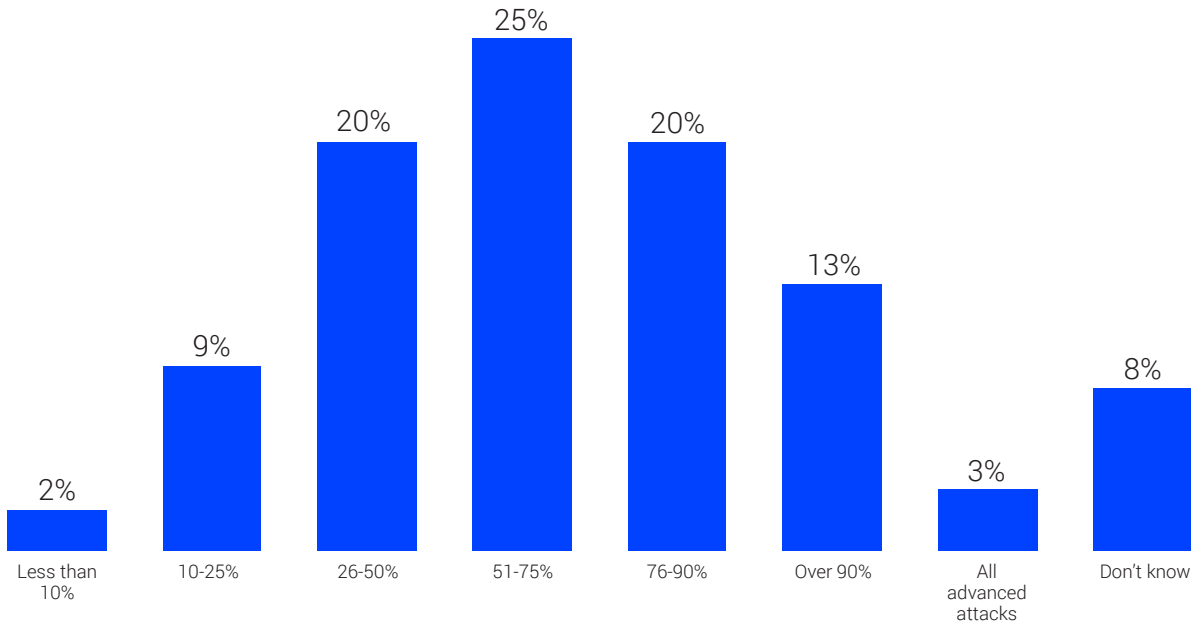
# Strategy

## Creating a smart detection strategy

### What are infosecurity workers using to stay protected?

Using their current security tools, only 3% of IT professionals reported that 100% of advanced attacks can be efficiently detected and isolated — proving there is always room for improvement!

**Using your current security tools, what percentage of advanced attacks can be efficiently detected and isolated?**

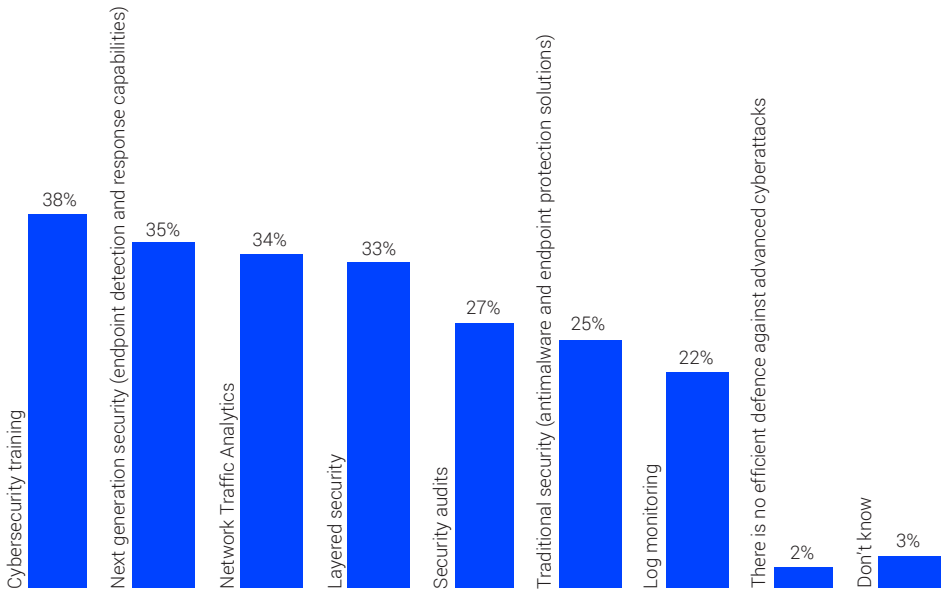


# Strategy

## The drivers behind infosec changes

Data protection is still the biggest driver for improving organisational cybersecurity, but do businesses keep themselves safe both now and into the future?

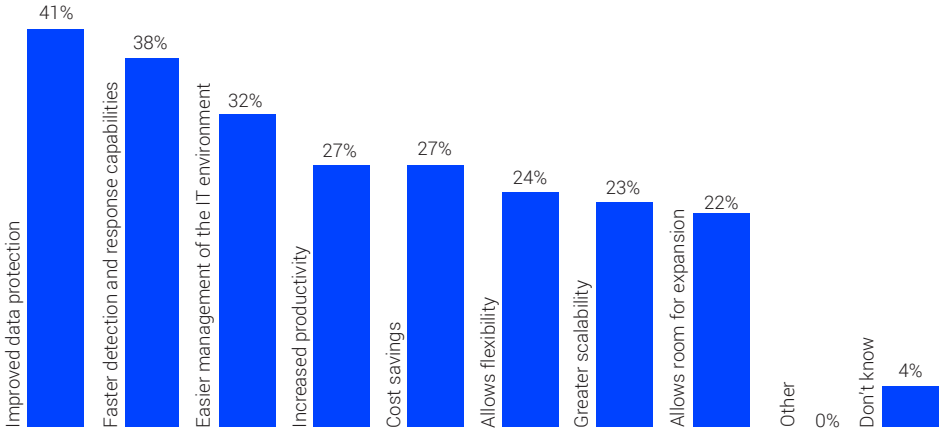
**What do you think is the best security defence approach against advanced attacks in your organisation?**




IT professionals place the most emphasis on training (38%), next-gen security solutions (35%) and network traffic analytics (34%) in regards to defending against advanced attacks on their organisation.

Unsurprisingly, improved data protection remains the main driver (41%) for IT professionals enhancing their company's cybersecurity posture. This is followed by faster detection and response capabilities (38%) and easier management of the IT environment (32%).

**What are the main drivers for enhancing your company's cybersecurity posture?**

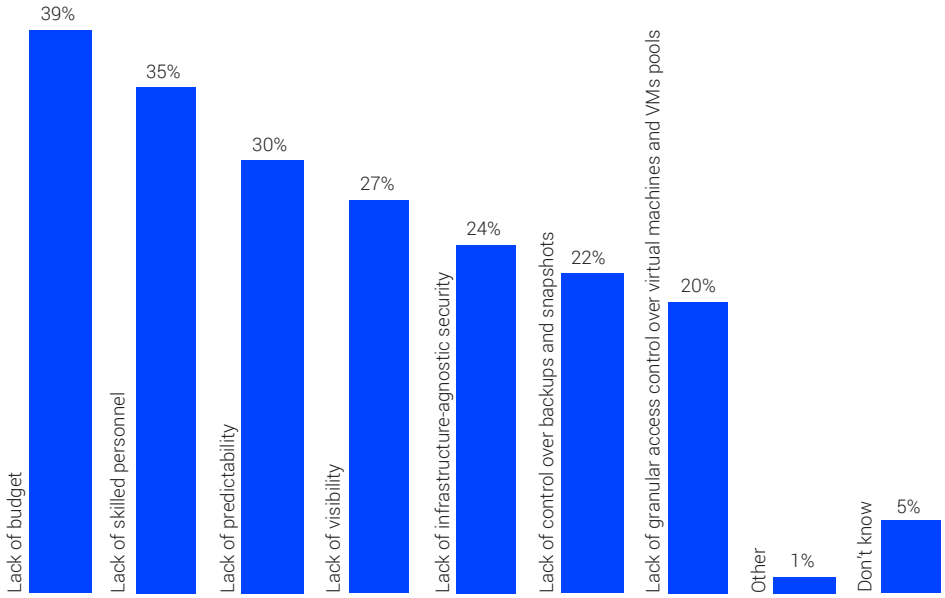


# Strategy

## The real cost of cybersecurity

### Are budgets reflecting the increase in awareness of cybersecurity best practice and strategy?

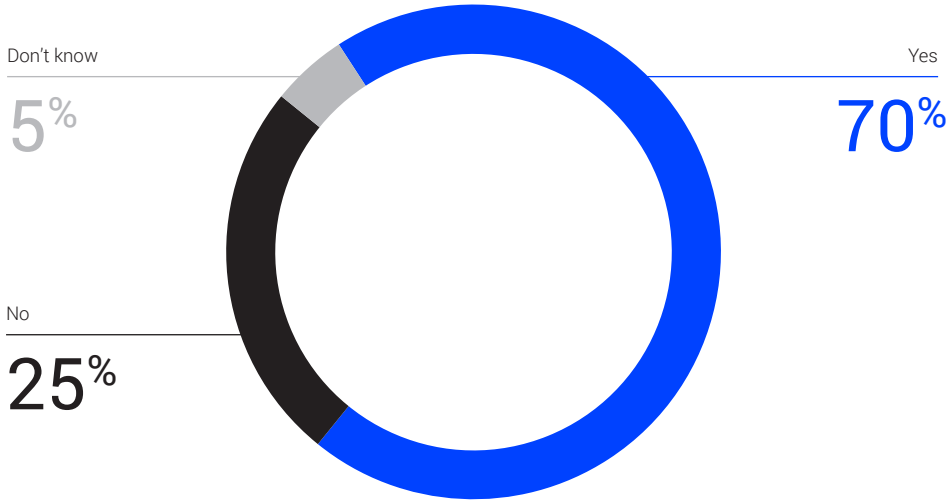
**What are the main obstacles to strengthening your company's cybersecurity posture?**




A lack of budget and skilled personnel again come up top in regards to being some of the main obstacles to strengthening company cybersecurity posture, at 39% and 35% respectively.

Encouragingly, over two-thirds (70%) of organisations are providing ongoing infosecurity training and support to their staff.

**Is your organisation providing ongoing infosecurity training and support?**



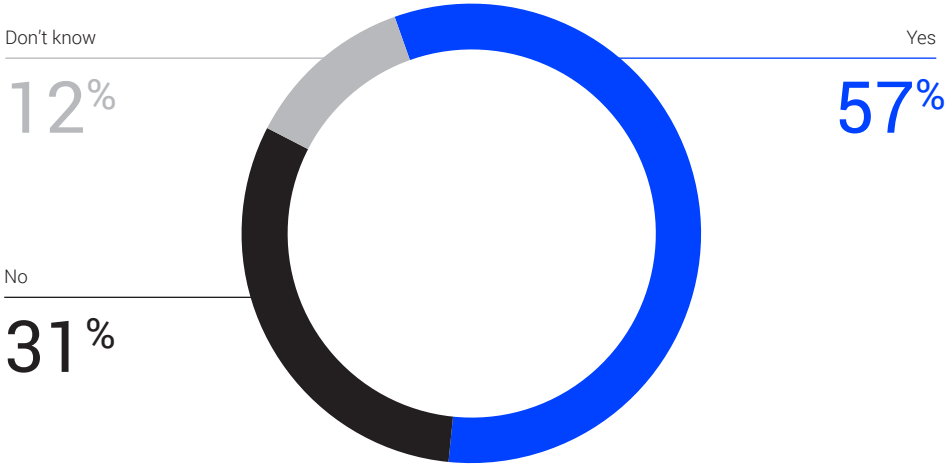
# Strategy

## The real cost of cybersecurity

Despite the increase in awareness of cybersecurity best practice and the greater emphasis on strategy, are budgets reflecting this?

Additionally, around three in five (57%) organisations have a dedicated budget for incident investigation and forensic (EDR).

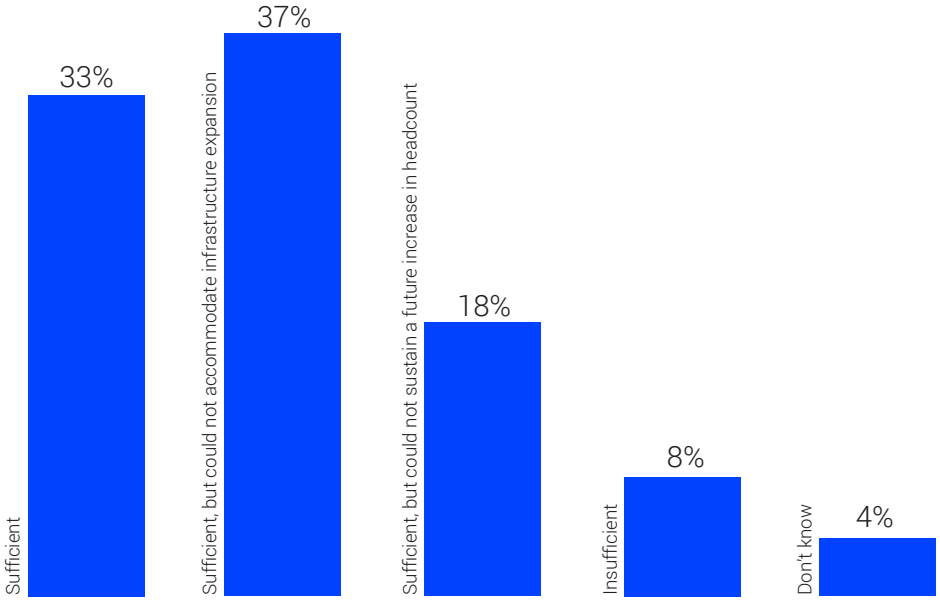
**Does your company have a dedicated IT security budget for incident investigation and forensic (EDR)?**




Over half (55%) of infosec professionals believe their IT security budget, while sufficient, could not accommodate an expansion of infrastructure or workforce.

Nearly three-fifths of small and medium-sized businesses (59%) believe their IT security budget is sufficient, but it could not accommodate an expansion of infrastructure or workforce.

**How would you rate the IT security budget of the company you work in?**



# To conclude

# Conclusion

"Organisations which have experienced breaches are on high alert. Infosec professionals that have experienced such an incident since 2017 are more likely to be kept awake worrying about it happening again. They also produce detailed reports on previous, and identified, cyber attacks more regularly. However, it's not all doom and gloom — as the overall amount of breaches to happen across organisations in the last three years has continued to reduce."

"Smaller companies have greater challenges, in particular around cybersecurity skills and knowledge, as well as detecting and isolating cyber attacks. While security operations centres (SOCs) can make a big difference in larger organisations — the cost of maintaining such a resource can sometimes be prohibitive for companies with smaller headcounts. In these instances, automated security solutions can go a long way to help bridge the talent gap."

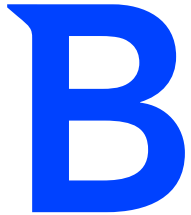
"The stresses and strains on security professionals are starting to show, with just over half (53%) having considered leaving their current role due to being under-resourced, both financially, and in terms of staffing. While budgets are always likely to be in flux, the lack of talent in the infosecurity space does signal the widening skills gap issue. By placing more emphasis on training and support for existing employees — organisations can at least go some way to alleviating talent pressures."

**Liviu Arsene, Global Cybersecurity Researcher at Bitdefender**

# Conclusion

"People want to get their jobs done, but this shouldn't be at the expense of poor cybersecurity hygiene — especially at the top of the tree. Concerningly, senior management is a main offender at flouting infosec rules with 57% either pushing back on or completely disregarding the rules. This makes them the most 'at risk' for departmental data breaches according to their infosec colleagues. Business decision makers should be leading by example; otherwise, it'll be them that have to pick up the pieces when disaster strikes."

"Infosec professionals believe that the best way of defending against advanced cybersecurity attacks is to provide adequate training (38%). This is proved by the fact that organisations providing info security training & support are better at detecting attacks quickly, and are more efficient at isolating them. In addition, cybersecurity executives are placing increased emphasis across next-gen security solutions (35%) and network traffic analytics (34%) to keep their organisations safe and secure."



"With an average of 53% of EDR alerts being false alarms and 29% of infosec professionals saying that it would take a week or longer to detect an advanced cyber attack, there's clearly a need for improvement in dealing with potential threats. This is where a next-gen EDR solution can help, such as Bitdefender GravityZone Ultra. Unlike other endpoint security solutions whose poor prevention makes them noisy and complex to operate, Bitdefender has developed over 30 layers of protection for all endpoints, offering the world's most effective protection integrated with low overhead EDR and Endpoint Risk Analytics (ERA) in a single agent, single console architecture."

**Bogdan Botezatu, Director or Threat Research at Bitdefender**

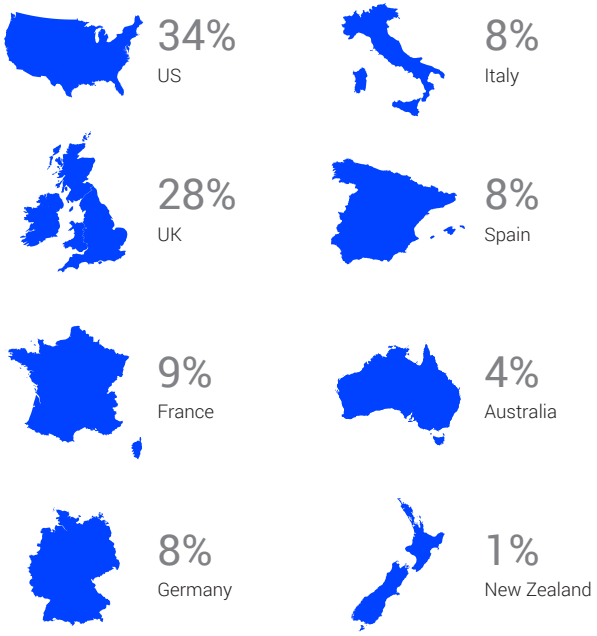
# Survey Method

The Bitdefender Hacked Off! Study was conducted among 6086 IT workers in July 2019 across the UK, US, Australia, New Zealand, Germany, France, Italy and Spain. Representing a broad cross section of organisations and industries, from fledgeling SMEs, through to publicly listed 10,000+ person enterprises. The report details the pressures faced by IT professionals, how these pressures impact the effectiveness of security measures, as well as analysing the best strategies to keep organisations safe.

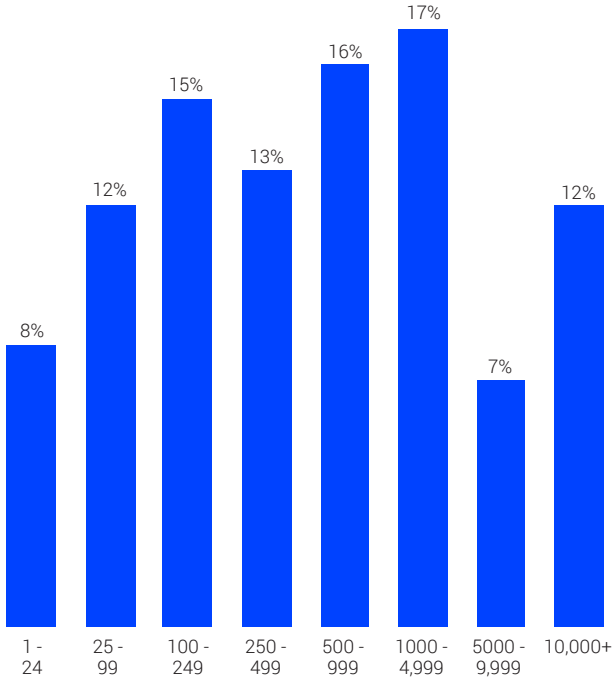
All audience members utilise and/or have decision-making power over data security solutions and software security products.

The interviews were conducted online by Sapio Research in July 2019 using an email invitation and an online survey.

**Respondents by geography**

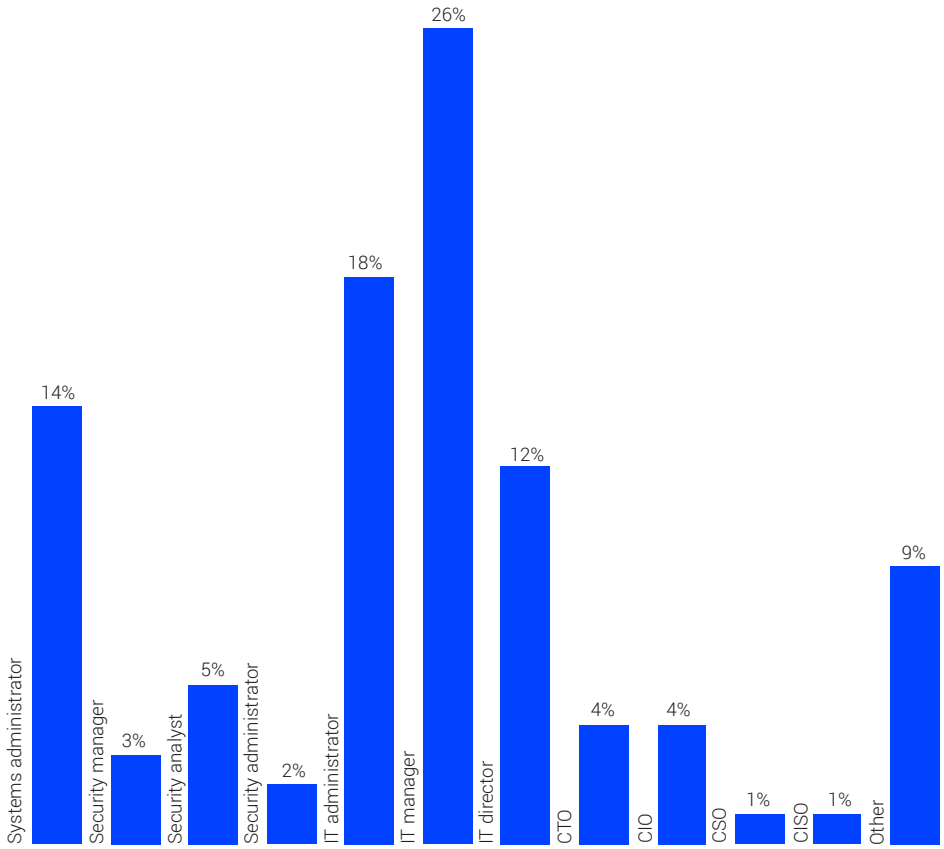



**Respondents by number of employees**



# Survey Method

**Respondents by geography**




**Respondents by number of employees**

| | | | | | |
|---|---|---|---|---|---|
| 2% | Agriculture | 4% | Government | 1% | Recreation |
| 1% | Apparel | 5% | Healthcare | 4% | Retail |
| 3% | Biotech | 1% | Hospitality | 1% | Shipping |
| 2% | Chemical | 2% | Insurance | 25% | Technology |
| 4% | Construction | 1% | Legal | 3% | Telecom |
| 6% | Education | 6% | Manufacturing/ Automotive | 2% | Transportation |
| 9% | Electronics | 3% | Media & Entertainment | 1% | Utility |
| 1% | Energy | 1% | Not-for-Profit/ Third sector | 2% | Other |
| 5% | Finance | 1% | Pharmaceuticals | | |
| 1% | Food & Beverage | 5% | Professional Services | | |

## About Bitdefender

Bitdefender is a global security technology company that provides cutting edge end-to-end cybersecurity solutions and advanced threat protection to more than 500 million users in more than 150 countries. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology and is a provider of choice in both hybrid infrastructure security and endpoint protection. Through R&D, alliances and partnerships, Bitdefender is trusted to be ahead and deliver robust security you can rely on.

## Contact Us


**bitdefender.com**

**800 388 8062**

**publicrelations@bitdefender.com**

**twitter.com/Bitdefender_Ent**