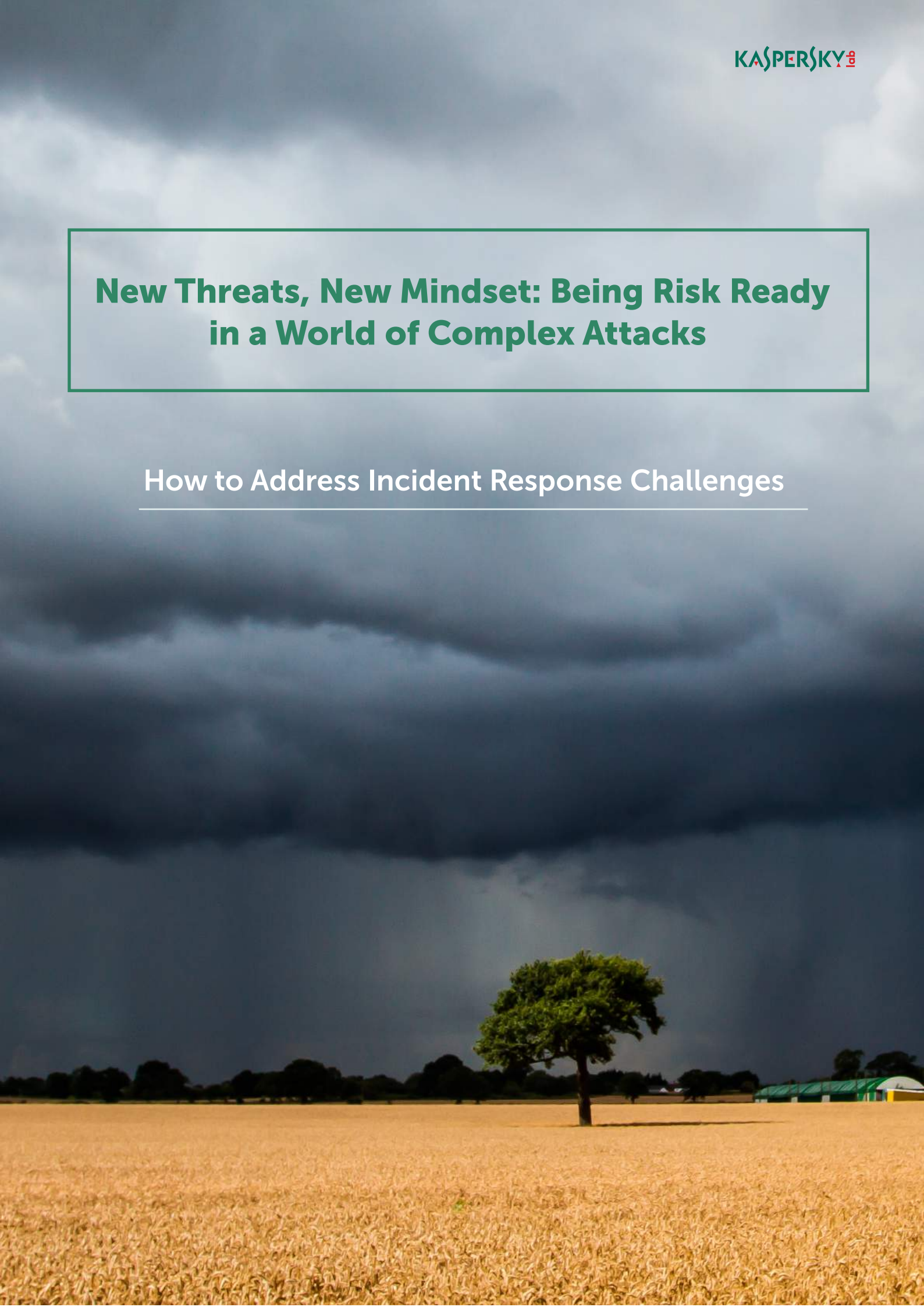


New Threats, New Mindset: Being Risk Ready in a World of Complex Attacks

How to Address Incident Response Challenges

Introduction

This year, Kaspersky Lab's quarterly threat reports highlighted significant developments in the world of advanced attacks and epidemic outbreaks, with the infamous WannaCry and ExPetr attacks dominating headlines the world over. Today, as well as having to cope with a near-constant deluge of traditional malware, businesses are also at risk of facing more sophisticated threats that often involve fileless malware, ransomware, reconnaissance activities and social engineering techniques. Such cunning attacks are usually multi-layered operations that may not even involve any malware at all, allowing them to easily slip undetected through endpoint protection solutions, leaving companies with a false sense of security when cybercriminals leave no footprint or destroy almost all traces of their activity.

Apparently, endpoints are still the main entry point for attackers and traditional prevention strategies used by companies are no longer adequate. With a security breach now more a question of 'when', not 'if', businesses need to rethink their approach to managing corporate security, putting more focus on 'always-on' monitoring and analysis leveraging threat intelligence, as well as mitigating an incident's consequences. It is now impossible for companies to fix and block everything, meaning frameworks need to be put in place that enable constant investigation and regular evaluation to ensure response strategies are up to date. Cybersecurity, therefore, is no longer a destination, but a continuous journey.

In such an environment, incident response becomes a complex organizational process that requires strategy, advanced cybersecurity technologies and input from many people within the organization. It demands a fast, efficient approach to assessing the vast volumes of security data generated by today's rapidly evolving threat landscape. The days of being able to manually respond to alerts and generate a complete picture of security are long gone, causing a 'millions of alerts' problem for IT security departments. Combined with an industry-wide skills shortage, this can result in the most crucial incident indicators being missed by overwhelmed security teams while the attackers slip undetected into the corporate infrastructure and remain there, undiscovered, to spy, steal or damage.

To help businesses navigate through today's cyberthreat landscape and address the organizational challenges and strategies of minimizing risks and responding to attacks, Kaspersky Lab carried out a study investigating the top concerns in the industry and the real incidents that businesses have faced in the last 12 months. The findings are summarised in the following report.

Methodology

The Kaspersky Lab Corporate IT Security Risks Survey is a global study of IT business decision makers, carried out by B2B International on behalf of Kaspersky Lab in April 2017.

The research questioned 5,274 workers about various aspects of cybersecurity, including their company's attitudes towards the area, the main challenges they are facing and the types of approaches/strategies they currently use.

Respondents represented very small businesses (1-49 employees), small to medium sized businesses (50-999 employees) and large organisations with 1,000+ employees. Results were compared to last year's survey - as well as between regions, industries and company sizes - to paint a comprehensive picture of the threat landscape.

Key Findings

- Targeted attacks have become one of the fastest growing threats in 2017, increasing in overall prevalence by 6% compared to 2016 and by 11% for enterprises. Comprising of not just common malware, but a unique malicious pattern that cybercriminals are using on organizations, a targeted attack is extremely dangerous for companies that rely solely on conventional approaches to cybersecurity.

- As there's no such thing as a common approach to fighting complex threats, businesses are struggling to understand how to deal with targeted attacks, with 42% of respondents admitting that they are unsure of the most effective response strategy. Worryingly, this figure is significantly higher (63%) among respondents who are IT security experts.

- A lack of IT security experts, especially those with specific knowledge in SOC management, incident response and threat hunting, is aggravating the situation. Half of businesses (50%) admit that they need to hire more experienced IT security professionals and a shortage of internal dedicated staff increases exposure to targeted attacks by 15%.

- However, organizations are reluctant to increase their security spend on protection against targeted attacks: 78% of respondents think they are currently spending enough, or even overspending, when it comes to investing in advanced threat defence.

- Meanwhile, there is a clear need for security solutions that go beyond prevention, as speed of detection is critical when it comes to the cost of breaches. When attacks were detected immediately, the average cost of recovery was $63K for SMBs and $102K for enterprises, compared to $465K and $1.2m respectively if detection took more than one week.

- Finally, efficient incident response is not just about technology. To be able to effectively combat complex cyberthreats, organizations need to think about it as a process, not a destination. In addition to the right technologies, the strategy should also involve human expertise (in house or outsourced), incident investigation frameworks, procedures and cost-efficiency planning.

Targeted attacks: An uphill battle

It's no secret that IT security teams have had their hands full over the last 12 months, highlighted by the fact that over three quarters (77%) of businesses reported that they experienced some kind of incident during this period.

Indeed, all types of attacks have increased in prevalence over the past year, with targeted attacks specifically showing one of the biggest overall increases (6%).

This is placing a huge amount of pressure on security teams, with many facing the dilemma of how to incorporate a response strategy that is able to protect their organizations against complex cyberthreats, without impacting business processes.

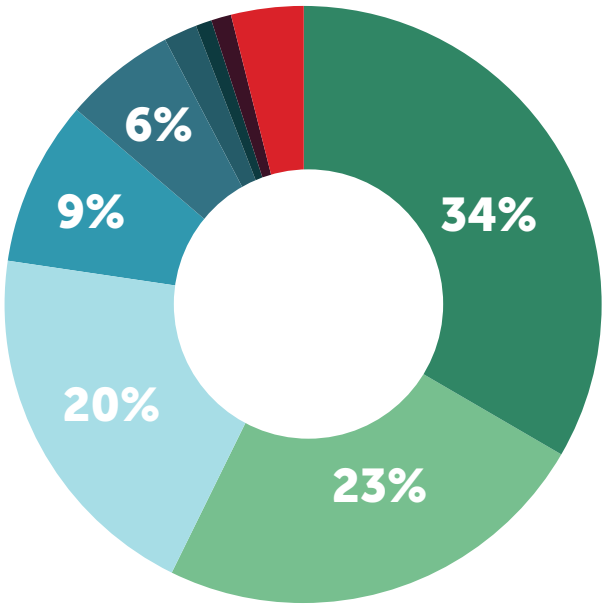
Data breaches are no longer a question of if, but when

Over a quarter (27%) of businesses admit that they have experienced targeted attacks on their infrastructure, up from 21% this time last year, and 33% of businesses feel that they are being specifically targeted by cyberattacks.

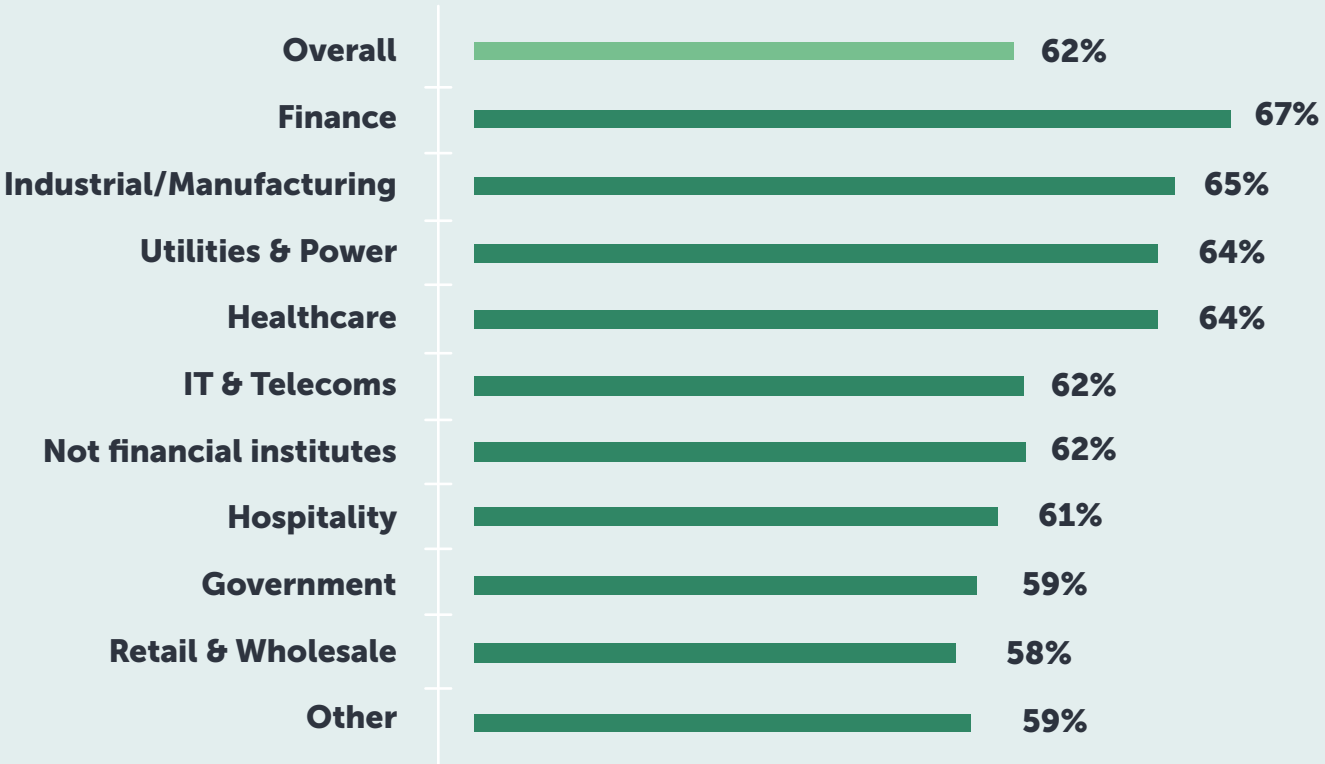
As you would expect, large organizations have experienced the highest number of targeted attacks, most likely due to the treasure-trove of sensitive corporate data that enterprises today hold, while organisations in the IT and telecoms (30%), healthcare (30%) and utilities (29%) industries have received the most interest from cybercriminals.

But it's not just the quantity of incidents that is causing problems for businesses. Two-thirds of respondents (66%) agree that IT security threats are becoming more complex, with 62% saying that they have experienced complex IT security incidents in 2017, as cybercriminals continue to develop their skillsets.

Complex security incidents experienced



None	34%
1 incident	23%
2 to 3	20%
4 to 5	9%
6 to 20	6%
21 to 50	2%
50 or more separate incidents	1%
Too many to guess	1%
Don't know	4%



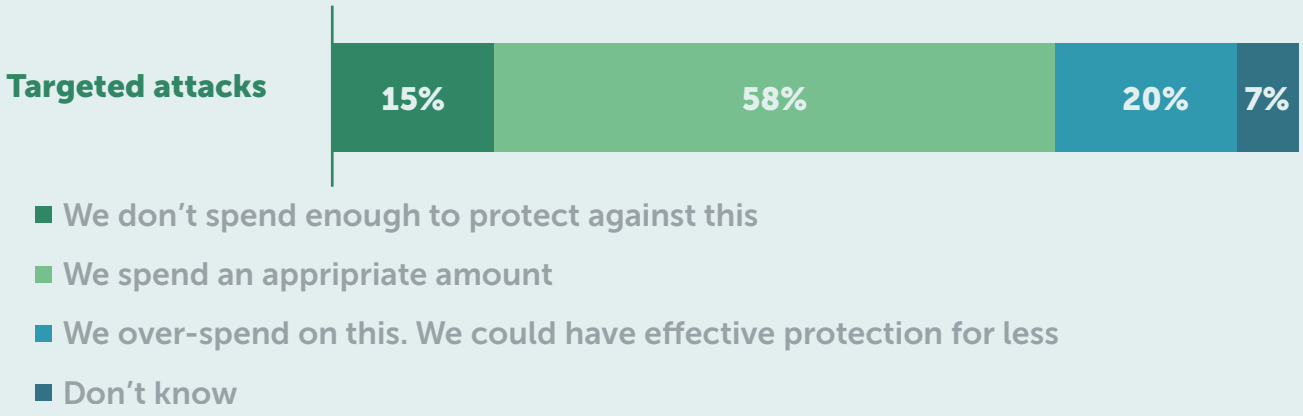
Source: IT Security Risks Survey 2017, global data

As a result, organizations are waking up to the fact that cybersecurity breaches are now inevitable. Indeed, 57% of companies believe that their organizations will be compromised at some point, up from 51% in 2016, suggesting that mindsets are changing when it comes to cybersecurity and highlighting a need to be able to effectively respond to any attack.

However, despite this awareness of the threats, businesses are still reluctant to increase their security spend, potentially due to being repeatedly told to buy new solutions to counter the "next big threat".

As the chart below shows, just 15% of businesses don't think they spend enough on protection against targeted attacks.

Attitudes toward investiment in protection from advanced threats



Source: IT Security Risks Survey 2017, global data

With regards to targeted attacks specifically, the vast majority (84%) of C-level IT specialists believe their company is either spending enough or over-spending on protection.

Interestingly, this figure is slightly lower (79%) among C-level executives in non-IT roles, suggesting that they are either more concerned about the business risks related to targeted attacks.

When it comes to responding to an attack, confusion reigns

A significant challenge facing businesses in today's cyber-battle relates to a lack of knowledge and expertise, which is making it harder for businesses to put clear response strategies in place.

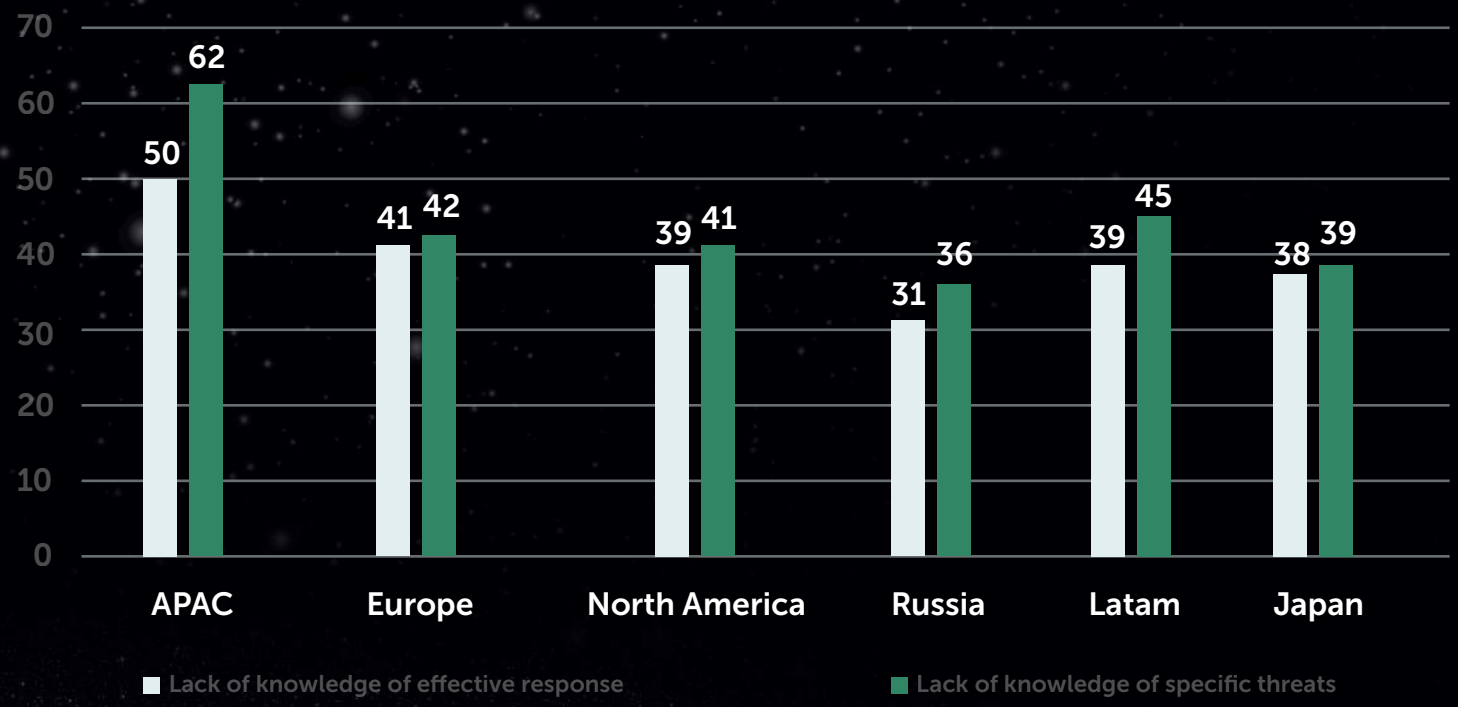
When asked, 42% of respondents agreed that their organization is not sure of the most effective strategy to combat threats like targeted attacks. This figure is higher for businesses in the healthcare (46%) and manufacturing (47%) sectors, possibly suggesting that firms in these industries are overwhelmed by the threat posed by such incidents.

There are also some geographical differences. Half of businesses in the APAC region agreed that they were unsure of the best response strategy, compared to 41% in Europe, 39% in North America and just 31% in Russia.

Similarly, 46% of respondents agreed that their knowledge of IT security threats specifically targeting their business is far from ideal, rising to 62% in APAC and dropping to 42%, 41% and 36% in Europe, North America and Russia respectively.

Businesses today cannot afford to be complacent when it comes to their cybersecurity, so need to ensure that an effective response strategy involving a combination of procedures, technologies and human experts is in place for when an attack does occur.

Cybersecurity expertise



Source: IT Security Risks Survey 2017, global data

Need for speed

One key issue the research highlights is the importance of speed when it comes to detecting and responding to data breaches and targeted attacks.

As well as the speed of detection being one of the strongest drivers of overall cost, rapid remediation is key to limiting the costs related to long-lasting reputational damage such as lost business, increased insurance premiums and embarrassing compensation bills.

But, according to the research, just a quarter (25%) of companies discovered their most serious security incident within a day, highlighting the importance of a comprehensive incident response process. Worryingly, it took every tenth company a year to discover the loss, theft or damage of data, making remediation a more complicated and expensive process.

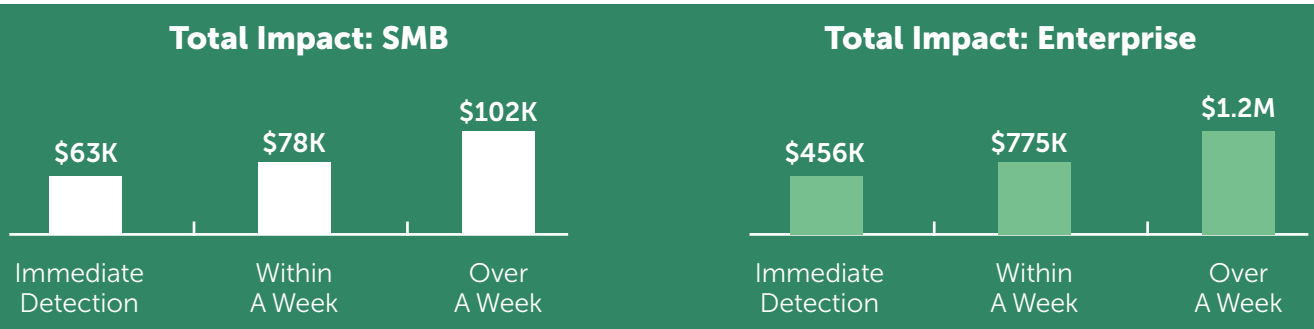
Time until discovery	Percentage
More than a year	5.9
About a year	10.3
Several months	16.6
Several weeks	18.3
Several days	22.9
Within a day	12.3
Within a few hours	8.7
Almost instantly	3.6

Source: IT Security Risks Survey 2017, global data

Government organisations were the quickest out of the blocks, with 34% detecting their most serious security incident within a day, compared to utilities where discovery took a year or more in 21% of cases.

This difference is likely due to a combination of reasons, including the pressures government organisations face when it comes to protecting data, the emphasis placed on security generally and the complexity of internal network architectures.

And it certainly pays for businesses to be on the ball, as detection speed has a significant material impact on the financial cost of an attack. For SMBs, the average cost of recovering from a targeted attack if it is detected immediately is $63K. This figure then jumps to $78K if detected within a week and $102K if detection takes longer than one week.



Source: IT Security Risks Survey 2017, global data

For enterprises, the increase is even more substantial, with a targeted attack costing an average of $1.2M if it remains hidden for more than a week – three times higher than the $456K cost for immediate detection.

Equally essential as detection is remediation, which is particularly important in limiting the long-term reputational and financial damage associated with a cyberattack.

Factors such as lost business, employing external professionals, training employees and paying extra for PR to repair brand damage all come into account, potentially adding hundreds of thousands of dollars onto the recovery bill and making a quick response even more important.

Skills shortage makes businesses slow and unsteady

So, why are businesses being slow to detect and respond to targeted threats? The simple answer is that there is just too much noise. With businesses facing an ever-growing number of attacks, security teams are struggling with an inability to spot the most dangerous threats through hundreds of thousands – if not millions – of incident alerts.

Over half (52%) of businesses admitted that it is becoming more difficult to tell the difference between generic attacks and truly serious threats, meaning targeted attacks are likely to slip through the cracks and cause severe damage. Clearly, a comprehensive response strategy is vital.

A lack of IT security expertise is further aggravating the issue. The cybersecurity skills shortage has been a widely-discussed issue, highlighted by the proportion of businesses that have been forced to turn to external help when recovering from a data breach.

Source: IT Security Risks Survey 2017, global data

Nearly three-fifths (58%) of respondents said a cyberattack forced them to employ the services of IT security consultants, suggesting a lack of in-house talent. Interestingly, there were notable geographical differences. In Japan, for example, 65% of businesses hired external consultants, whereas the figure was significantly lower for organisations in Europe (54%) and Russia (40%).

Healthcare (65%), telecoms (63%) and finance (63%) were the industries most likely to look for help externally, while retail and government organisations were more likely to rely on existing staff.

Total Financial Impact For SMBs	**$91K**	**$86K**
Total Financial Impact For Enterprises	**$1.1M**	**$930K**
Presence Of Internal Specialists	**No**	**Yes**

Source: IT Security Risks Survey 2017, global data

Finally, 53% of businesses agreed that they need to employ more specialists with specific experience in IT security rather than general IT professionals – a figure which jumps to 61% for enterprises. This is a worrying trend, as having internal IT security specialists gives businesses a financial edge when it comes to responding to data breaches.

It also highlights the importance of incorporating a combination of people, processes and technology into any effective incident response strategy.

Proactive protection: The answer to targeted attacks

All of these trends are combining to form something of a perfect storm of cyberthreats and IT security professionals have started to accept that a change in attitude is required to combat them.

Businesses are realising that, in order to gain visibility through the sea of alerts and react immediately to the most severe threats, a proactive 'detection and response' mindset is the best way forward.

Nearly three-fifths (59%) of businesses believe their IT security strategy should prioritise being able to more effectively detect and respond to attacks, with the finance (66%) and utilities (63%) industries leading the way.

This mindset is especially prevalent in large enterprises with more than 1,000 employees (62%), possibly due to the sheer quantity of attacks impacting such organisations and a more mature understanding of the modern threat landscape.

There is also a clear need for security solutions that go beyond prevention and provide a more complete cybersecurity package. For example, 56% of businesses agreed that they need better tools to detect and respond to advanced persistent threats (APTs) and targeted attacks and 67% of companies consider solutions that continuously and proactively seek threats and threat actors that are targeting their organizations to be effective.

Countries in Europe appear to be particularly in favour of this approach, with 75% of companies in Italy, 71% in Spain, 70% in France and 69% in the United Kingdom in agreement. At the opposite end of the spectrum are the United States (60%) and Japan (55%).

Finally, an attitude in favour of proactive detection and response is endorsed by those in IT, as 60% of IT personnel believe in the effectiveness of services that proactively seek threats that are targeting their organisation, compared to 47% of non-IT staff.

Businesses are clearly ready to change their thinking regarding effective security strategies. The challenge is creating an efficient process which makes use of technology and people to help organizations stay one step ahead of the attackers.

Conclusion

The rapid and constant development of the cybersecurity landscape means businesses simply can't afford to stand still when it comes to protecting themselves against sophisticated, targeted attacks, one of the fastest growing threats in 2017.

Security solutions are generating more incident alerts than ever before and overstretched IT teams are understandably finding it hard to cut through the noise, meaning the most dangerous threats are often slipping through the cracks. This, combined with the rapid increase in recovery costs as threats remain undiscovered and the fact that threats are getting more complex, is putting businesses on the back foot.

Clearly, something needs to change. 57% of respondents to our survey agreed that an attack is going to get through at some point, meaning organizations need to be able to paint a full picture of cybersecurity across the entire organization. This will also enable businesses to adapt their approach and focus on being able to immediately detect and respond to threats, as opposed to the more traditional mind-set of focusing just on prevention.

IT security departments, as the technology gatekeepers, have a responsibility to lead this evolution by making sure their organizations continue to invest in advanced technologies and professionals with specific knowledge and experience in threat hunting, forensics and incident response.

However, as protection from modern threats is a complex process, these components must be supplemented by effective recovery procedures and a comprehensive incident investigation framework, comprised of always-on monitoring, advanced detection and critical security event mitigation.

In today's world, businesses can never be completely risk free. But, by shifting their focus towards proactive protection, adopting a strategic approach to security and planning in advance, they can get themselves into a position to be able to effectively respond to targeted attacks and contain the damage.