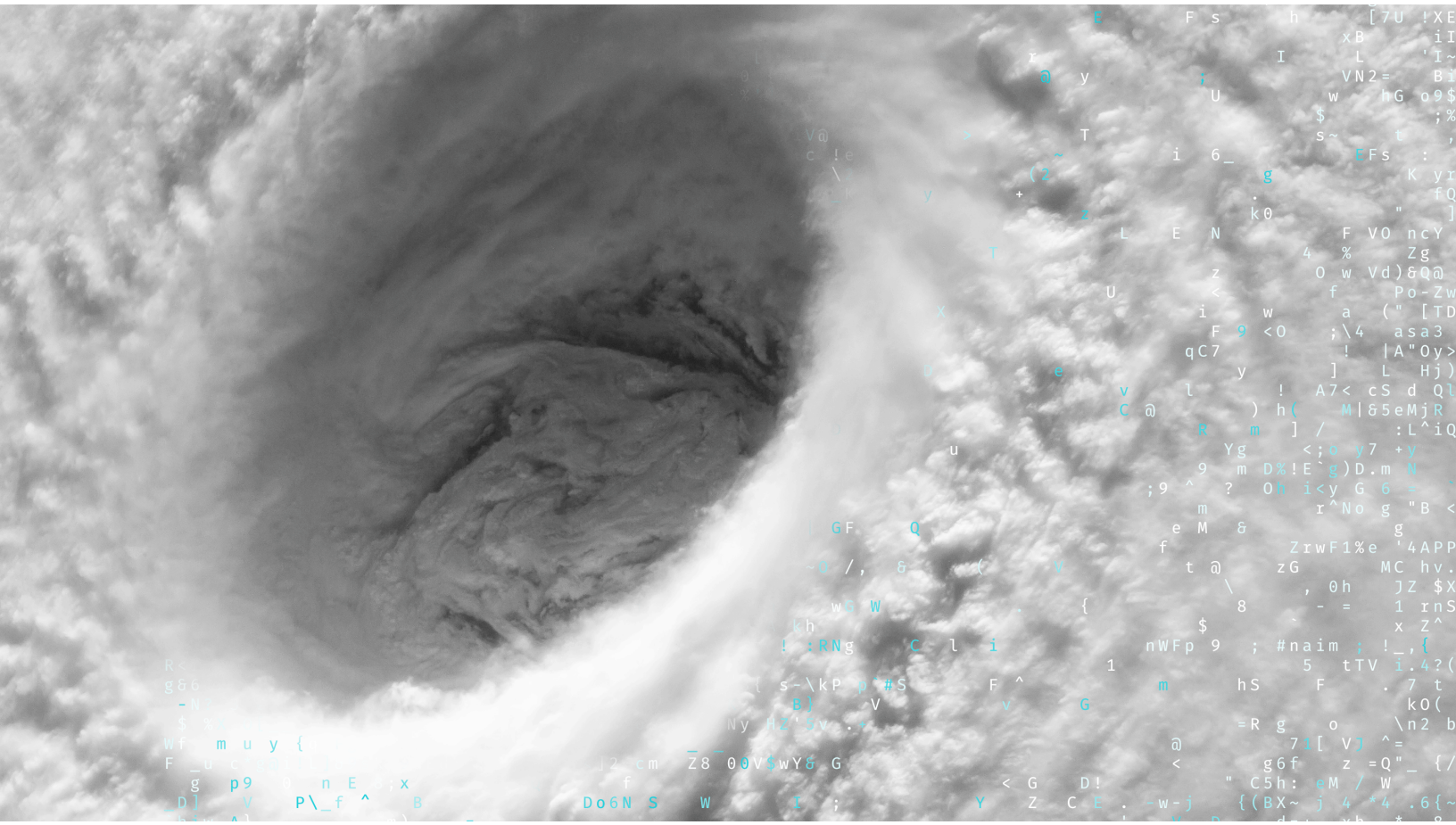
solarwinds msp

SURVEY RESULTS

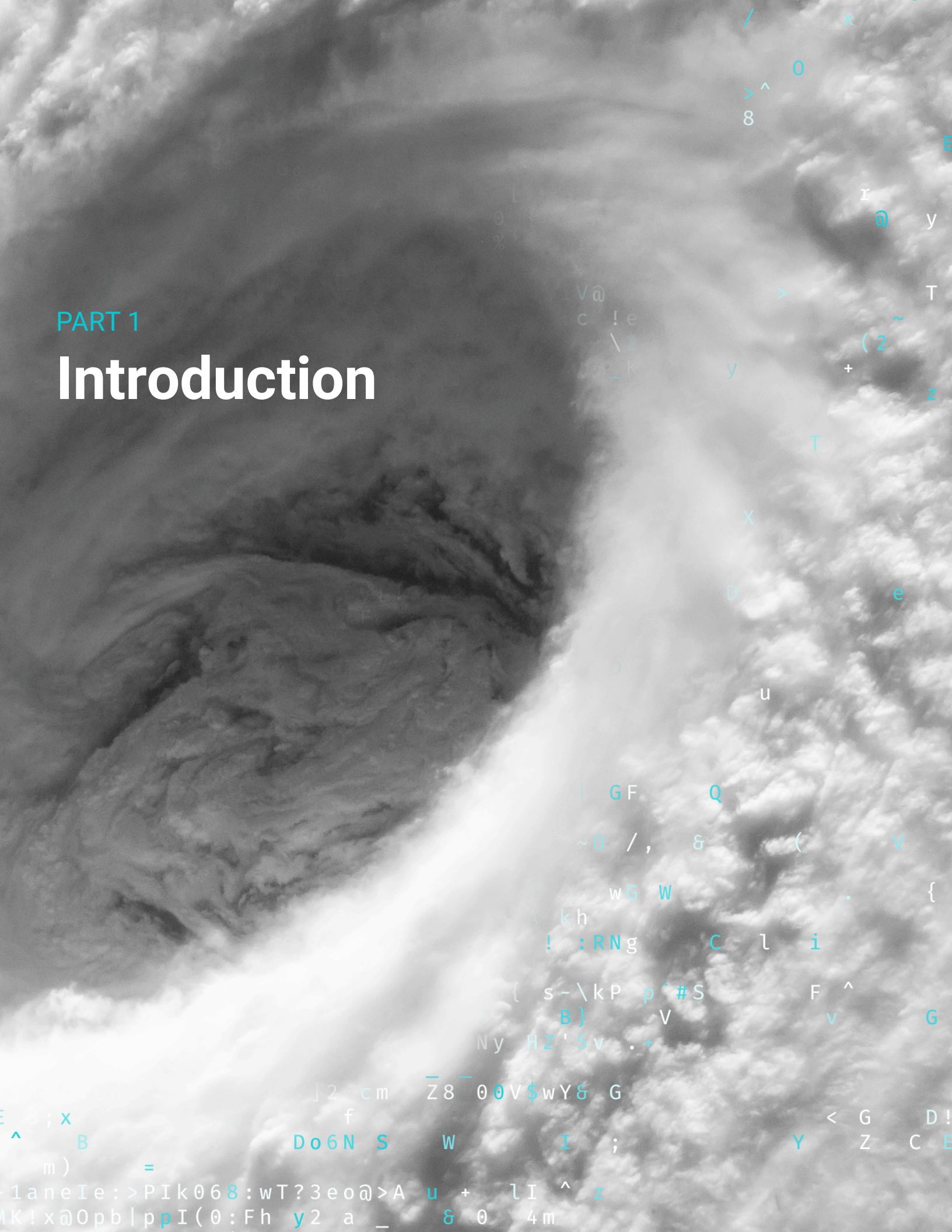
The 2017 Cyberattack Storm Aftermath

A Survey of IT Leaders' Thoughts on WannaCry, Petya, and Vault 7



Ponemon INSTITUTE

Sponsored by SolarWinds MSP
Independently conducted by Ponemon Institute, LLC
Publication Date: March 2018



PART 1

Introduction

Introduction

Ponemon Institute is pleased to present the findings of a study conducted to determine perceptions about recent ransomware attacks and the Vault 7 identified vulnerabilities and malware variants. The study involved 202 senior-level security executives in the United States (US) and United Kingdom (UK). According to the research, both US and UK respondents have very similar views about emerging cybersecurity threats that could negatively impact their organizations. Our research utilized diagnostic interviews with security leaders to obtain information about the following cybersecurity threats:

Vault 7: On March 7, 2017, WikiLeaks began its series of leaks on the US Central Intelligence Agency (CIA). Code named "Vault 7" by WikiLeaks, it is the largest ever publication of confidential documents on the agency. The disclosures revealed several variants of malware, created by the CIA, including Year Zero, Dark Matter, Weeping Angel, and HIVE, among others.

On April 14, 2017, the Shadow Brokers hacker group leaked an NSA-created vulnerability dubbed EternalBlue. Unlike the Vault 7 malware variants, which were not globally exploited, this variant was used to propagate the widespread ransomware attacks **WannaCry** and **Petya** at a massive global scale.

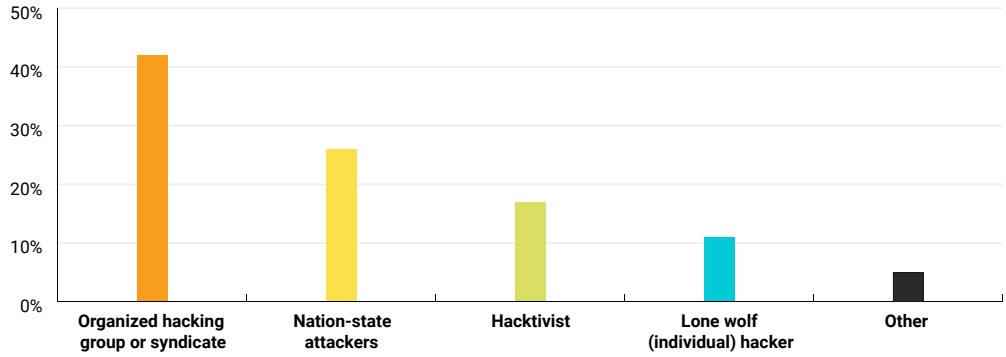
WannaCry: On May 12, 2017, the WannaCry ransomware spread around the world, affecting hundreds of thousands of targets, including public utilities and large corporations. Notably, it temporarily crippled National Health Service hospitals and facilities in the United Kingdom, creating chaos for many British patients.

Petya: On June 27, 2017, another wave of ransomware hit targets worldwide via Petya. The Petya attack was more advanced than WannaCry in many ways. It infected networks in multiple countries—such as the US pharmaceutical company Merck®, Danish shipping company Maersk®, and Russian oil giant Rosneft. The ransomware hit the Ukrainian infrastructure particularly hard, disrupting utilities like power companies, airports, public transit, and the central bank.

According to our research, senior-level security executives seem ill prepared to address the above-mentioned cybersecurity threats despite their perception that cybersecurity threats will increase over the next 12 months (53 percent of respondents). Specifically, many do not seem to have a firm understanding of ransomware and Vault 7-type attacks. Further, they admit that their organizations lack the ability to prevent or detect these attacks. When asked what cyberattacks present

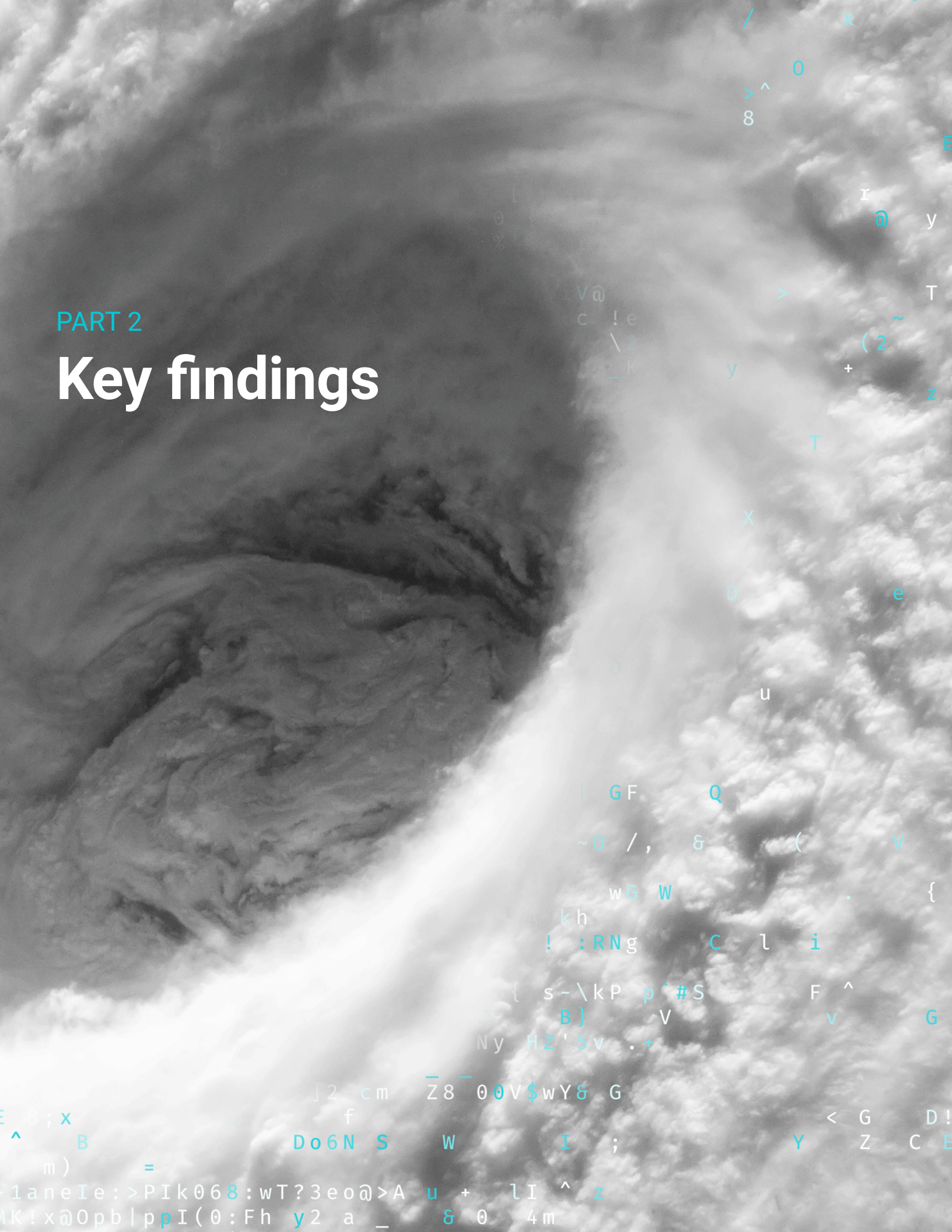
the greatest risk to their organization, 42 percent of respondents cite organized hacking groups, and 26 percent of respondents say the greatest risk is posed by nation-state attackers, as shown in Figure 1.

Figure 1. What cyberattacker presents the greatest risk?



ABOUT OUR EXPERT, TIM BROWN

Throughout this report, you will see callouts containing practical advice from Tim Brown, VP of security for SolarWinds MSP. Tim has over 20 years of experience developing and implementing security technology. Tim's experience has made him an in-demand expert, where he has met with members of the United States Congress, the United States Senate, and the White House. He also holds 18 security-related patents.



PART 2

Key findings

Key findings

In this section, we provide an analysis of the research findings. The complete audited findings are presented in the Appendix of this report. The following topics are covered in this report:

- Knowledge and understanding of cybersecurity risks
- Prevention and detection of cybersecurity threats
- Cybersecurity risk based on size, footprint, and industry
- Preparedness to address cybersecurity threats

KNOWLEDGE AND UNDERSTANDING OF CYBERSECURITY RISKS

First, we sought to answer two questions around both ransomware and Vault 7 attacks—how much do experts know, and how much risk do they perceive in these threats?

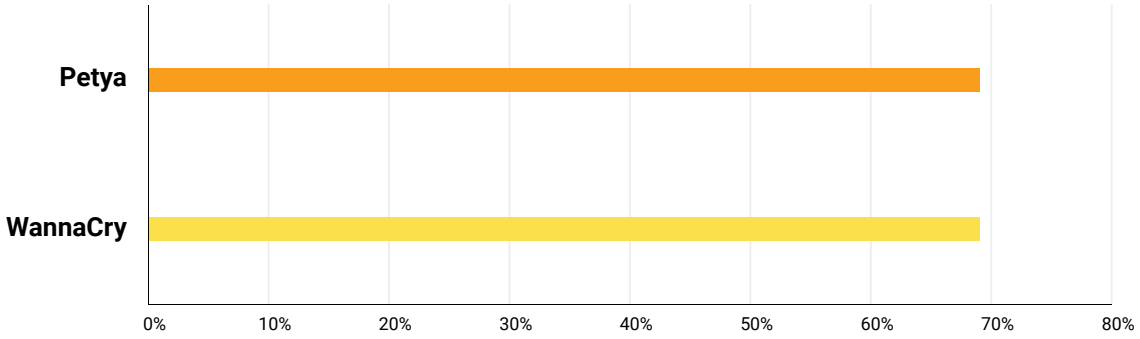
We broke this into two sections to understand:

- Their perspective on ransomware strains—specifically WannaCry and Petya
- Their perspective on Vault 7-style attacks

The key takeaway we found was experts were more aware of and perceived a greater threat from ransomware than they did with Vault 7.

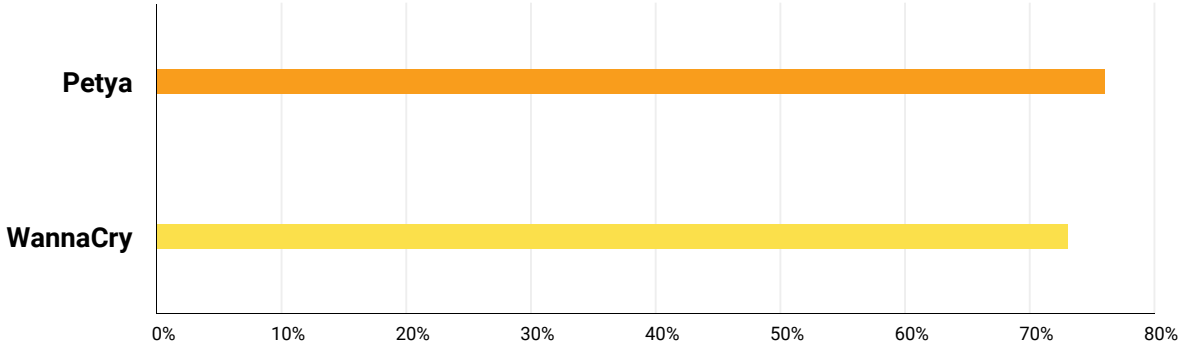
FINDINGS

Figure 2. Level of knowledge about ransomware attacks



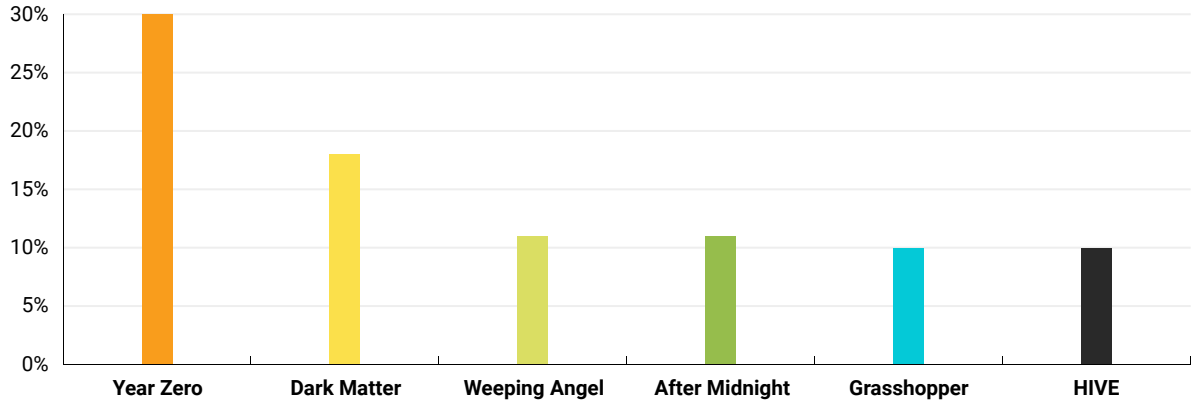
In Figures 2–6, we used a 10-point scale (1 = low knowledge to 10 = high knowledge). In Figure 2, we found that 69 percent of respondents possess a high level of knowledge regarding ransomware attacks, including Petya and WannaCry.

Figure 3. Level of risk for ransomware



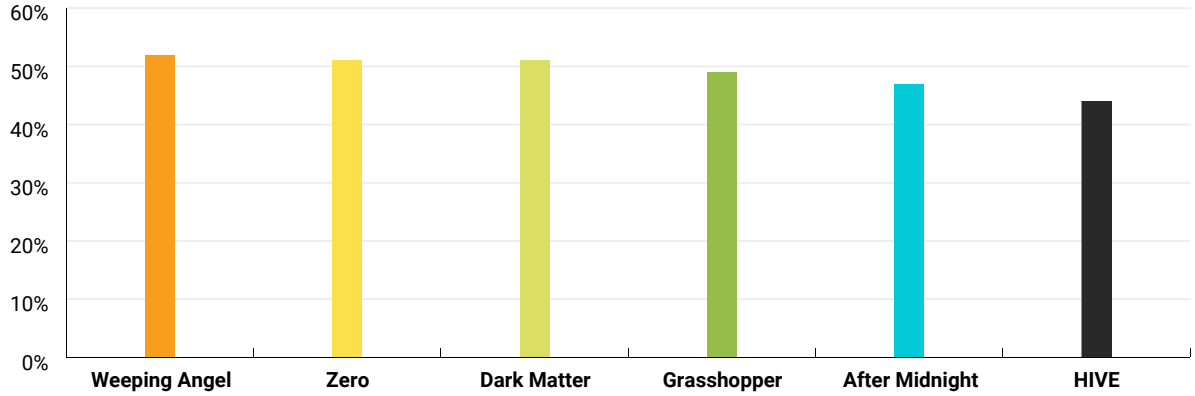
As shown in Figure 3, 76 percent rate the risk of Petya as very high and 73 percent rate the risk of WannaCry as very high.

Figure 4. Level of knowledge about Vault 7 components



In contrast, most respondents have a low level of knowledge and perception regarding the risk of Vault 7 attacks. In fact, the highest level of awareness was for the Year Zero variant for which 30% of respondents said they had a high level of knowledge, as shown in Figure 4.

Figure 5. Level of risk for Vault 7 attacks



According to Figure 5, respondents do not rank the risk of Vault 7 components as high as the risk of ransomware. About half of respondents rate the level of risk as very high for Vault 7 attacks, such as Weeping Angel, Zero, and Dark Matter.

The low level of knowledge about these threats might affect the respondents' perceptions about the potential risk.

PREVENTION AND DETECTION OF CYBERSECURITY THREATS

Next, we sought to understand how IT experts viewed their detection and prevention capabilities.

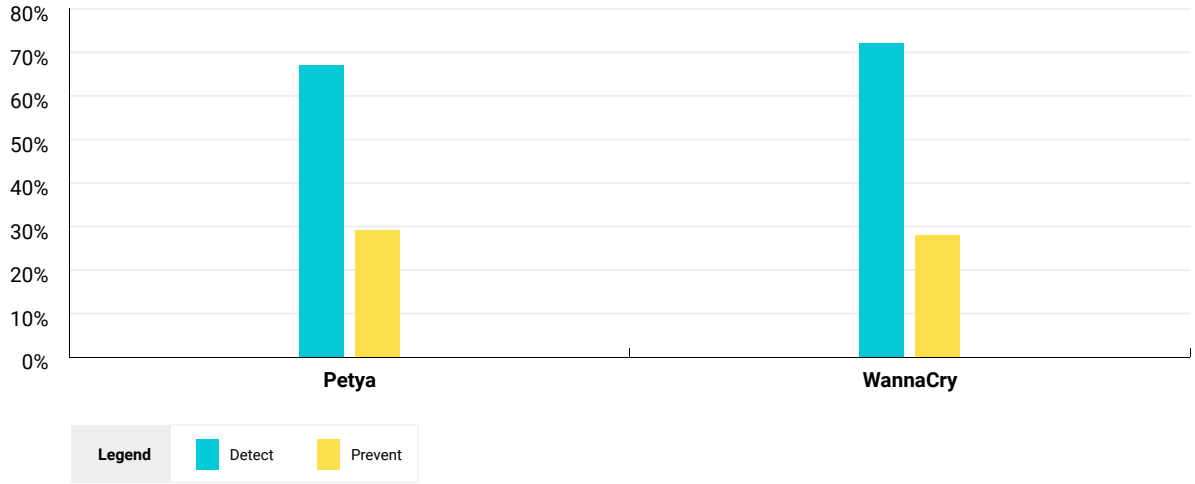
We focused on the following:

- How well can organizations detect and prevent both the WannaCry and Petya ransomware strains?
- How well can they detect and prevent Vault 7 attacks—and how does this compare to their abilities with ransomware?
- How many respondents experienced an exploit in the previous year, and for those that did, what were the consequences?

Because several of the 2017 attacks could have been prevented via security bulletins, we also asked respondents about their usage and knowledge of free notification tools like US-CERT.

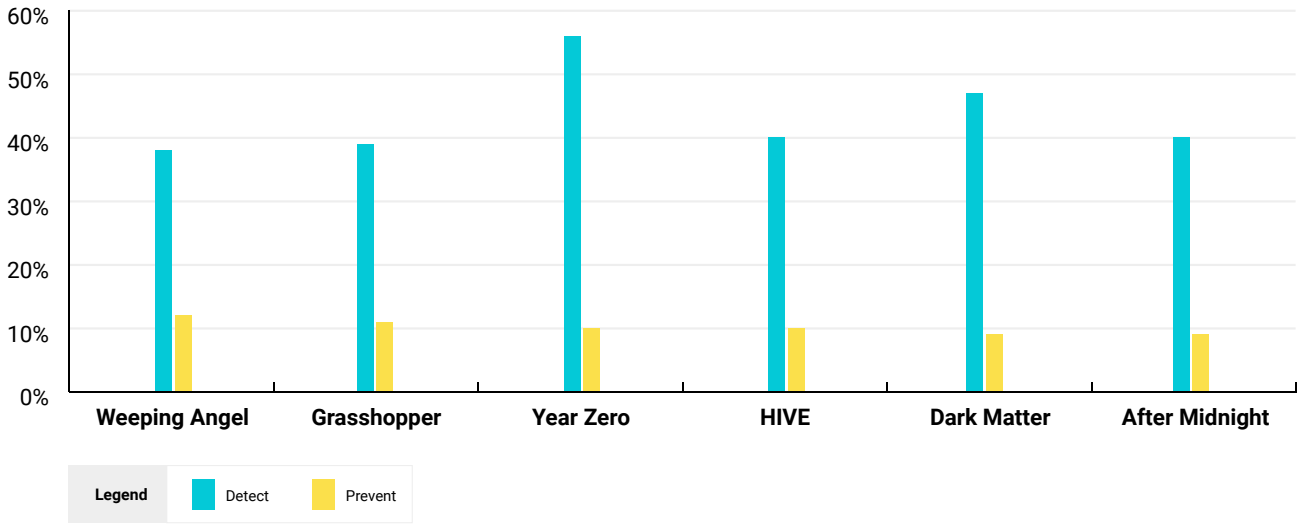
FINDINGS

Figure 6. Is your organization capable of preventing & detecting ransomware?



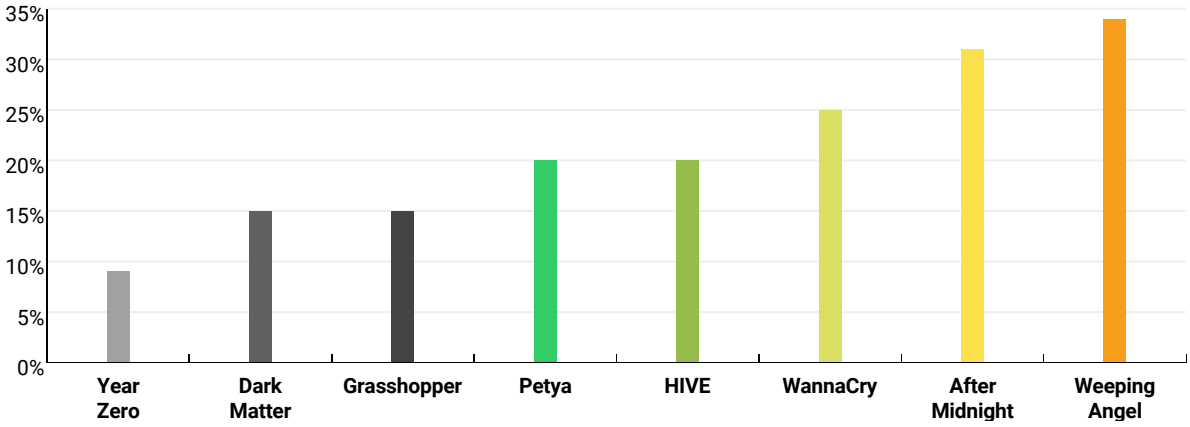
In Figures 6–7, we used a 10-point scale (1 = incapable to 10 = highly capable). **More respondents believe they can detect, but not prevent, ransomware attacks.** Only 29 percent of respondents acknowledged that they would be able to prevent a Petya attack, and 28 percent of respondents say they would be able to prevent a WannaCry attack. Sixty-seven percent of respondents believe they would be able to detect a Petya attack, while 72 percent stated their organization would be able to detect a WannaCry attack.

Figure 7. Is your organization capable of preventing & detecting Vault 7 attacks?



Their ability to prevent and detect a Vault 7 attack is rated lower than ransomware prevention and detection. Only 9 percent of respondents say their organization is capable of preventing an attack, such as Dark Matter or After Midnight, and only 38 percent of respondents say their organization is able to prevent a Weeping Angel attack.

Figure 8. Which cybersecurity threats were detected?



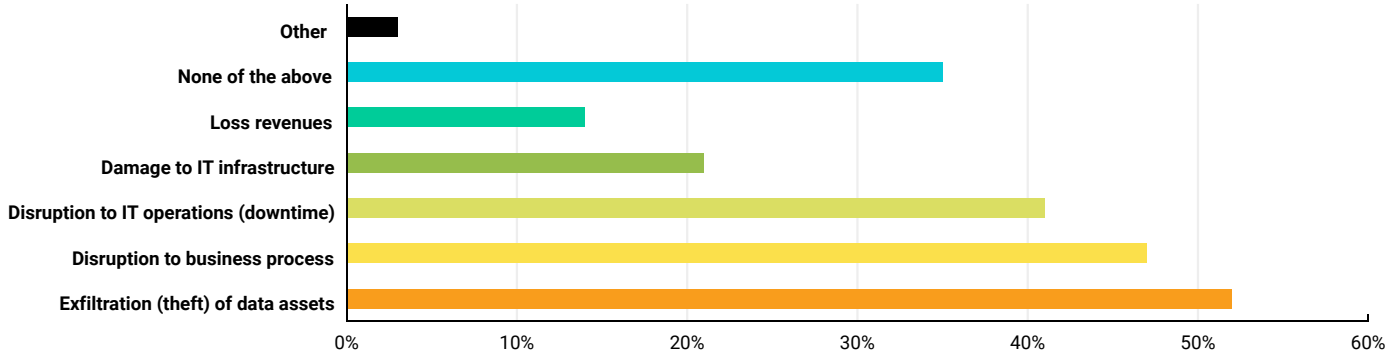
The majority of respondents admit their organizations experienced one or more of the above-mentioned cyberexploits or attacks during the past year. There is general consistency among respondents in terms of each attack's consequences, such as IT and business disruption and the loss of data assets. In Figures 8–9, more than one response was allowed.

Fifty-four percent of respondent companies detected one or more of the above-mentioned ransomware and/or Vault 7-type threats on their networks. The cybersecurity threats most often detected were Weeping Angel (34 percent of respondents) and After Midnight (31 percent of respondents). Twenty-five percent of respondents say their organization was able to detect the ransomware attack WannaCry. Of these organizations, 47 percent stated that they were unable to resist the attack.

EDUCATING CUSTOMERS ABOUT THE REAL THREATS

Media hype has created a lot of confusion, even among security professionals. For example, almost half of our respondents claim they have detected the Vault 7 threats listed in our survey. Indeed, more than a third (34%) claim to have detected Weeping Angel. However, it's unlikely these organizations would have been victim to that threat because it requires having physical access to a Samsung® TV and plugging a USB into it. By taking on the role of security expert, MSPs can guide organizations to help them take the right measures without getting caught up in the hype.

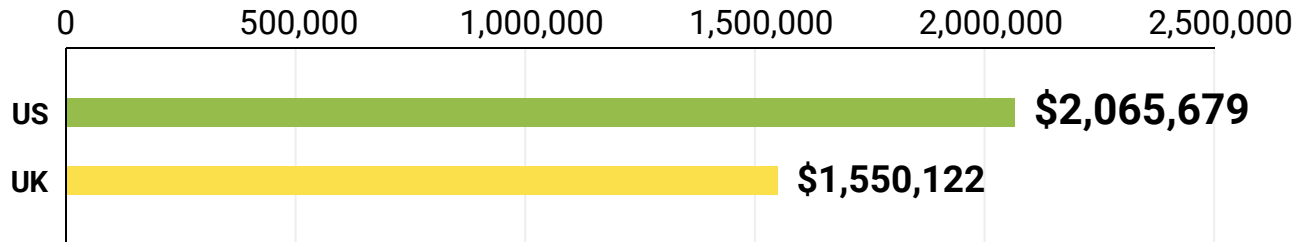
Figure 9. What was the consequence of the attack?



The theft of data assets and disruptions to business processes are the two most negative consequences of cyberattacks from the previous year. As shown in Figure 9, the results of cyberattacks included the theft of data assets (52 percent), disruption to business processes (47 percent), disruption to IT operations or downtime (41 percent), damage to IT infrastructure (21 percent), and loss of revenue (14 percent).

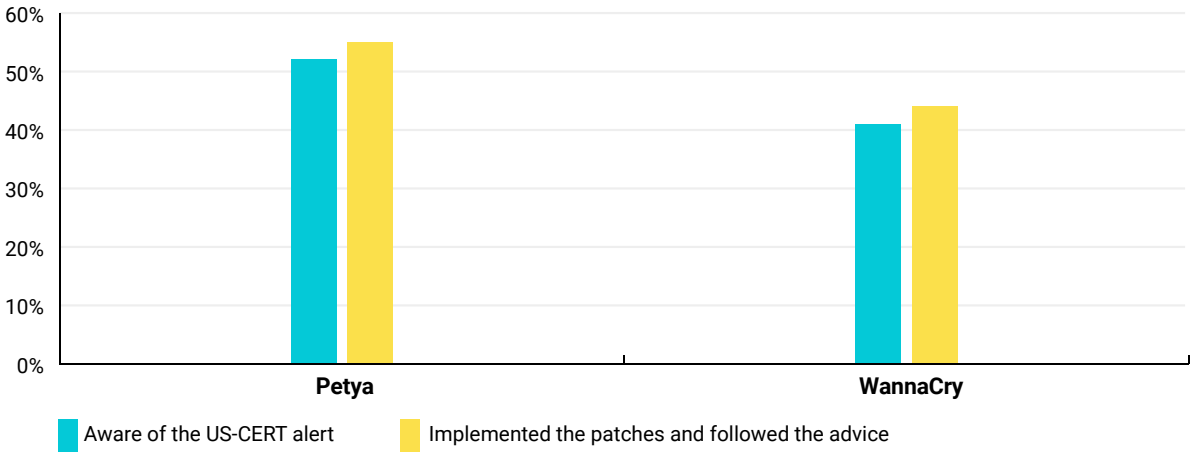
Figure 10. Economic damages to US and UK companies

US dollars



In Figure 10, the average cost incurred as a result of the above-mentioned cyberattack is shown in US dollars. The US companies (125) represented in this study incurred an average amount of $2.07 million USD and the cost to the 77 UK companies was $1.55 million USD.

Figure 11. Awareness about US-CERT alerts on Petya & WannaCry and implementation of patches



We also found that senior-level security staff do not utilize "free" intelligence sources, such as US-CERT, that might be helpful in identifying cybersecurity threats before they hit the organization. This is especially disconcerting given that a majority of respondents believe the risk level to their organization will increase over the next 12 months. It is possible, however, to obtain intelligence from paid sources, such as vendor feeds, that may be more robust than free sources like US-CERT. In addition, and perhaps even more concerning, many did not follow the subsequent patching recommendations.

Fifty-two percent of respondents were aware of a US-CERT alert on Petya, as shown in Figure 11. Only 41 percent recall receiving an alert about WannaCry from US-CERT. Fifty-five percent of respondents' organizations implemented the patches following the advice it received from US-CERT regarding Petya. Only 44 percent of organizations followed the advice about WannaCry.

MAKING PATCHING A PRIORITY

Patching remains challenging for many businesses. As a case-in-point, despite patches being made available to remediate the Petya and WannaCry ransomware attacks, 45% and 56% of respondents, respectively, did not implement them.

Infrastructure is becoming more complex, which means that keeping up-to-date on the number and types of patches available and necessary is a challenge for security professionals. Being proactive, rather than reactive, is crucial—and this is where MSPs can help.

Furthermore, regularly checking US-CERT updates and other valuable data sources can help MSPs stay proactive and be able to explain to their customers what the risks are, at a specific moment in time.

Being one step ahead of the game is fundamental for MSPs to protect themselves and their customers.

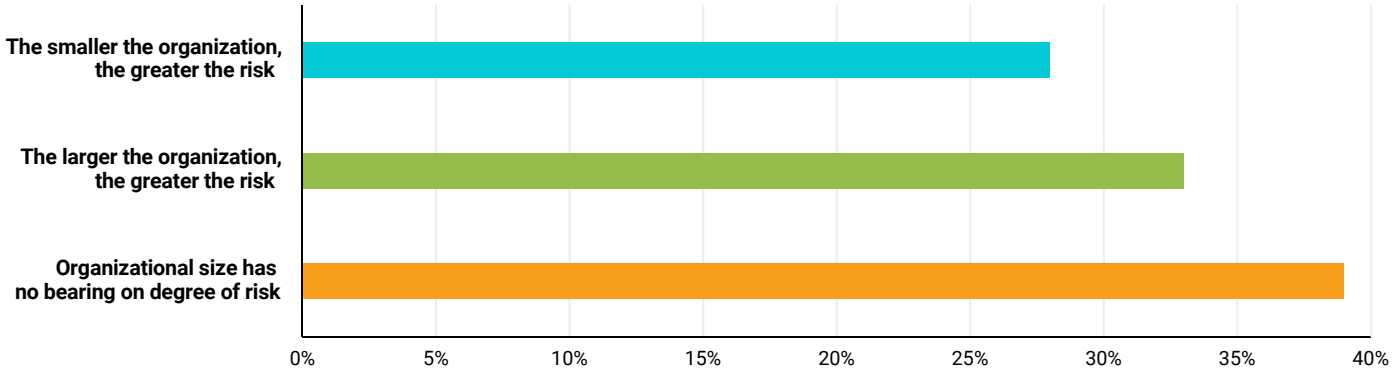
CYBERSECURITY RISK BASED ON SIZE, FOOTPRINT, AND INDUSTRY

Next, we sought to figure out which organizations were the ***most*** susceptible to cyberthreats. Attacks on large companies often get the lion's share of headlines, but hackers could just as easily shoot for small- and mid-sized businesses to get valuable data. To that end, we asked:

- Does size affect an organization's susceptibility to a cyberattack?
- Are private-sector or public-sector organizations more susceptible to a cyberattack?
- What role does the geographic footprint of an organization play?

FINDINGS

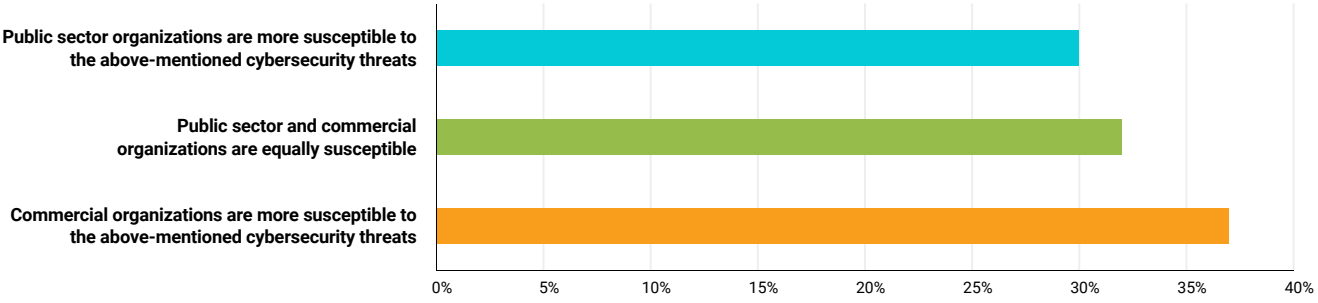
Figure 12. Are cybersecurity threats more dangerous based on the size of the organization?



There appears to be a lack of agreement among senior-level security professionals about the relationship between cyber-risk and certain exogenous factors. The findings in this section reveal perceptions about different levels of risk based on organizational size, geographic footprint, and government versus commercial infrastructure.

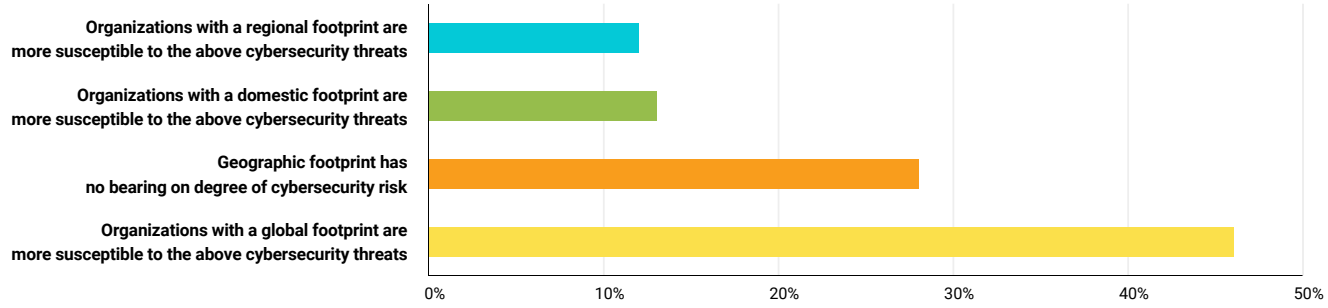
One-third of respondents believe that these above-mentioned cybersecurity threats are more dangerous to a larger organization. Another 28 percent believe smaller organizations face an increased level of cybersecurity risk, and 39 percent believe that an organization's size has no bearing on risk, as shown in Figure 12.

Figure 13. Are cybersecurity threats more dangerous to public sector than commercial?



According to Figure 13, 30 percent of respondents believe that the above-mentioned cybersecurity threats are more dangerous to public sector (governmental) organizations than commercial companies. Another 37 percent believe commercial organizations face a higher level of cybersecurity risk, and 32 percent believe that risk does not increase or decrease for public sector versus commercial organizations.

Figure 14. Does an organization's geographic footprint affect cybersecurity threats?



As shown in Figure 14, 46 percent of respondents believe that cybersecurity threats are more dangerous for organizations that have a global footprint versus a regional footprint (12 percent) or a domestic footprint (13 percent). Another 28 percent believe that an organization's geographic footprint does not impact risk.

UNDERSTANDING AN ORGANIZATION'S PROFILE

The size of an organization, its location, and geography have little impact on its vulnerability to cybersecurity threats. What's more important are the services it provides, the products it offers, and ultimately, the data it holds. A hospital or health service is a prime example here.

The size only increases the risk if the organization is a worthwhile target in the first place. In short, the profile of an organization determines the risk, while the risk determines the level of protection it needs and the services and solutions its MSP should provide.

To better protect them, MSPs need to ask their customers some key questions. What type of data do they hold or have access to? How complex are their organizations? Whom do they share data with? What would be the effect of a breach or compromise? What larger infrastructures/networks are they connected to? These "crown jewels" are all things cybercriminals will aim to exploit.

MSPs can help their customers more adequately prepare and defend against threats by focusing on good cyberhygiene that takes all of these critical factors into account.

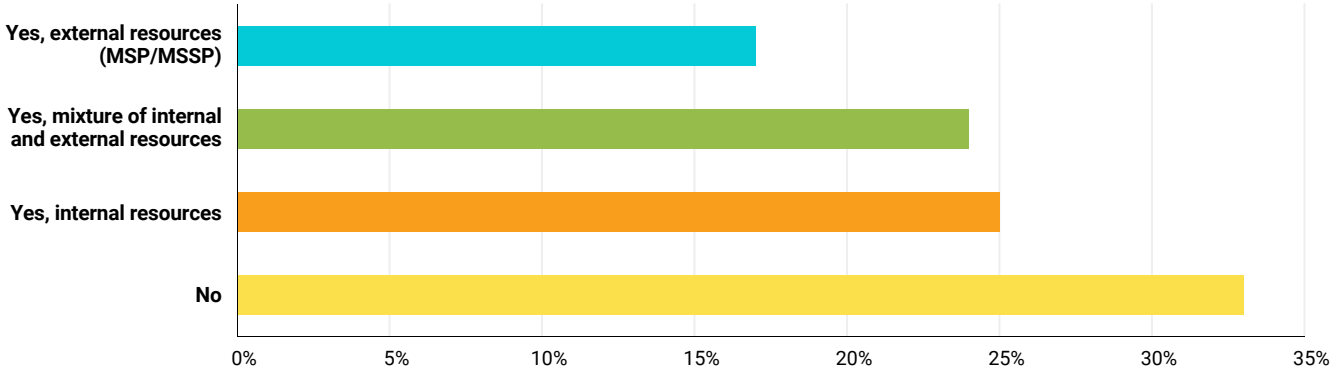
PREPAREDNESS FOR ADDRESSING CYBERSECURITY THREATS

With the amount of cyberattacks in 2017, we can surmise that cybersecurity will only become more important in 2018. To that end, we wanted to conclude our study by asking the IT experts to look ahead for the coming year. This section covers:

- Do these experts have the in-house staff expertise to tackle these threats?
- Do their organizations have sufficient technology to tackle these threats?
- Will they have enough security budget allocated in the coming year?
- How will the experts spend their budget—on internal activities, external resources, or a mixture of the two?

FINDINGS

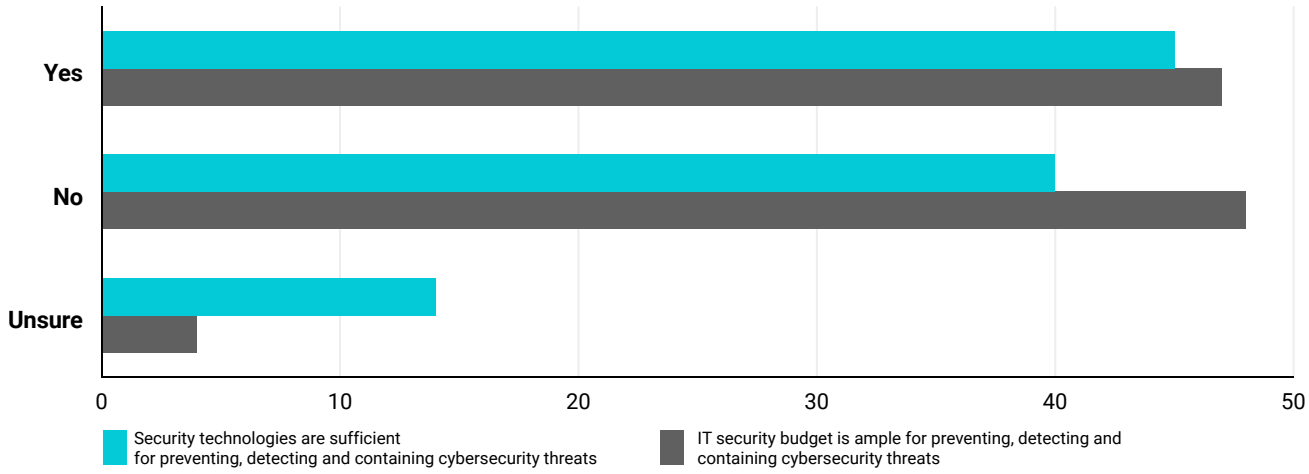
Figure 15. Does your organization have personnel who have the expertise to tackle cybersecurity threats?



Only a small minority of organizations has a full complement of in-house dedicated personnel. The shortage of IT security personnel is a systemic problem that many organizations face. Despite this shortage, an essential role and responsibility of the security leader includes the recruitment and retention of personnel, which appears to be difficult to accomplish.

As shown in Figure 15, 25 percent of respondents employ personnel (specialists) who have the expertise to tackle the above-mentioned cybersecurity threats. Another 17 percent engage outside resources such as managed security services providers (MSSPs), and 24 percent engage a combination of both external and internal experts. Thirty-three percent do not employ specialized personnel or engage outside experts.

Figure 16. Are technologies and budget sufficient for dealing with cybersecurity threats?

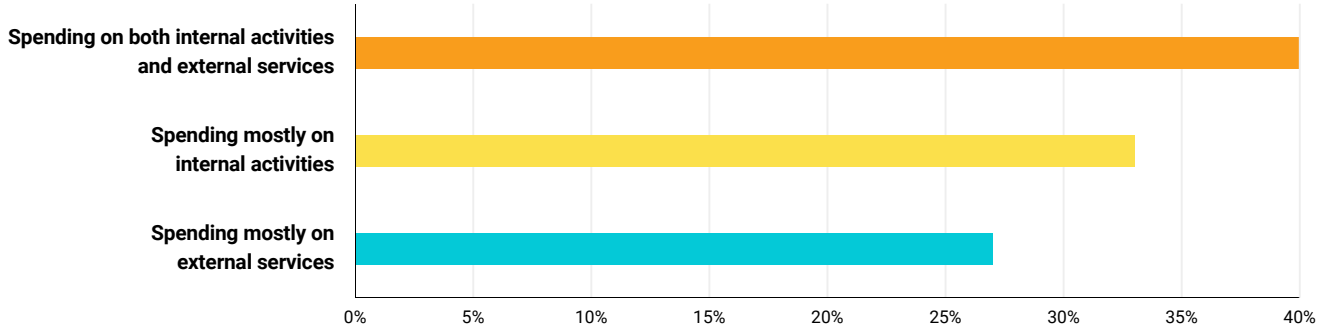


Less than half of respondents believe their organizations' enabling security technologies and budget are sufficient to prevent, detect, and contain risk. Taken together, these findings support earlier results that show a low rating by security leaders about each organization's ability to curtail cyberthreats, such as ransomware or Vault 7-type attacks.

According to Figure 16, 45 percent of respondents deploy enabling security technologies that are sufficient in preventing, detecting, and containing significant cybersecurity threats. Another 40 percent say their security technologies are not sufficient (and 14 percent are unsure).

Forty-seven percent of respondents believe their organizations' IT security budget is sufficient in preventing, detecting, and containing significant cybersecurity threats. Another 48 percent say their budget is not sufficient (and 4 percent are unsure).

Figure 17. Will budget focus on internal activities or external support (MSSPs)?



Many senior security professionals appear to have a favorable view of MSSPs. In short, the ability to outsource core IT security activities may be a smart move for organizations that do not have the in-house resources to minimize cybersecurity threats and risks.

For those respondents who say the budget is sufficient, 85 percent believe the IT security budget needs to either increase or significantly increase to keep up with emerging cybersecurity threats. According to Figure 17, one-third of respondents believe the budget increase will focus on internal activities, 27 percent believe the budget increase will focus on external activities, and 40 percent believe the budget increase will focus on a combination of internal and external activities or services.

For respondents who presently engage an MSSP, 45 percent believe this service provider is sufficient in preventing, detecting, and/or containing the significant cybersecurity threats. Another 44 percent say the service provider alone is not able to prevent, detect, and/or contain threats (and 11 percent of respondents are unsure).

THE PATH TO MSSP

The survey shows there is a huge opportunity for outsourcing security from both a people and technology perspective. A third of respondents stated they do not have the necessary expertise in-house to undertake cybersecurity threats, a result of both security staffing shortages and rising costs. And less than fifty percent have little faith in their enabling security technologies, a factor multiplied by people and budget challenges.

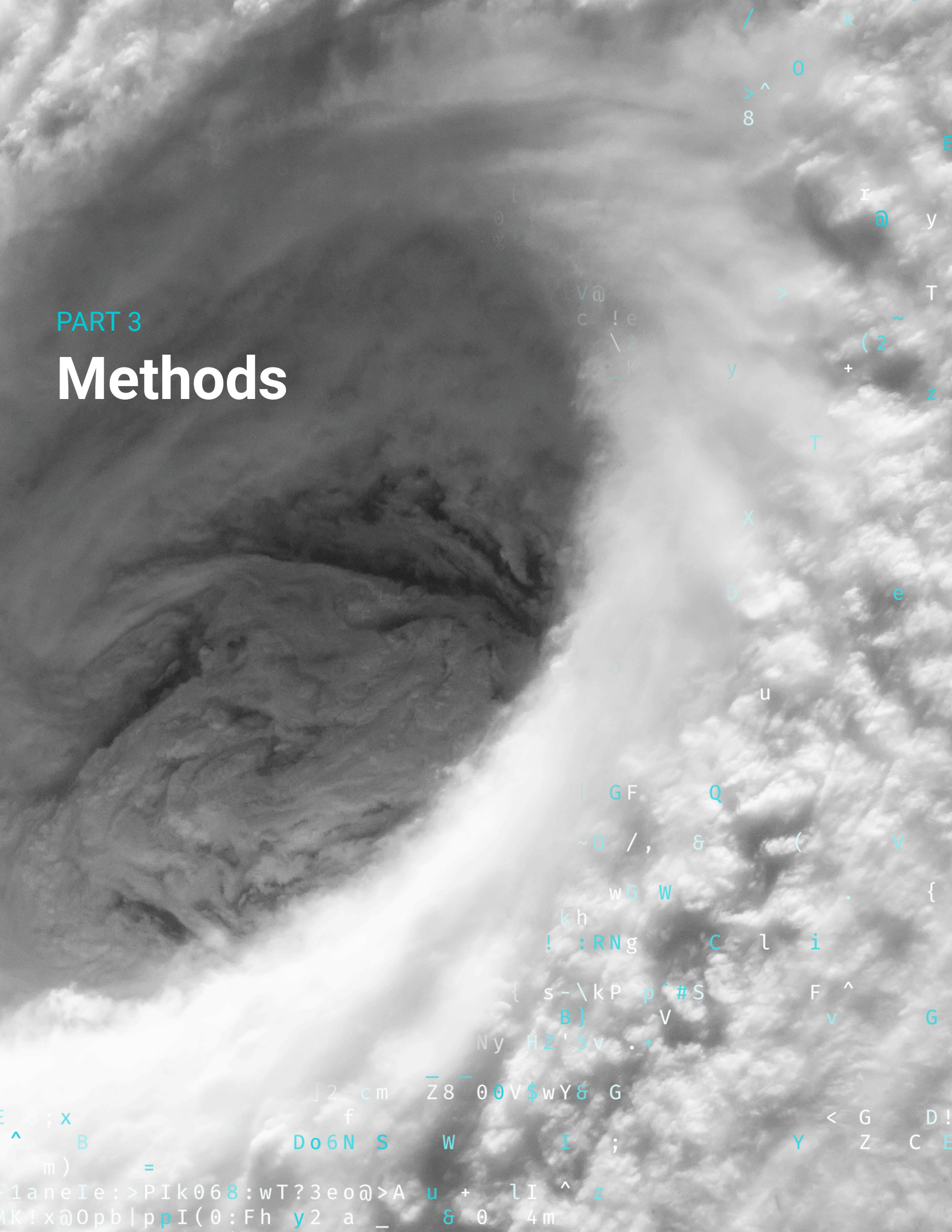
This is where MSPs shine. They have the power to deliver flexible and scalable security technology platforms and the people to support them, that many businesses—especially SMBs—don't. It's a win-win for everyone.

This doesn't mean the MSP has to do everything for everyone. All MSPs should be able to measure security risk and educate their customers about the risk they face. Some will focus on good cyberhygiene, while others will focus on more advanced offerings such as VCSO, PEN testing, and 24/7 monitoring.

The term MSSP should be considered as a tiered term. Some MSSPs provide a full range of security services, but an MSP providing good cyberhygiene services and utilizing partners for more advanced services should also consider themselves an MSSP. They are an active partner helping to manage the security for their customers. After all, in our latest "The Path to MSSP" research, 70% of the market confirmed they would look more favorably on a service provider that described itself as a MSSP.

Being responsible for providing the organization's IT, MSPs are a central component in reducing cyber-risks and should therefore take on a leadership role in risk management, education, and the intersection of business and security.

The opportunity for MSPs is there and will not go away any time soon, but it is important that they understand the multiple tiers from MSP to MSSP and know where they fit. Those that can adapt rapidly to improve their knowledge, skills, and resources in key areas and seize the MSSP mantle will quickly outrun their competition.



PART 3

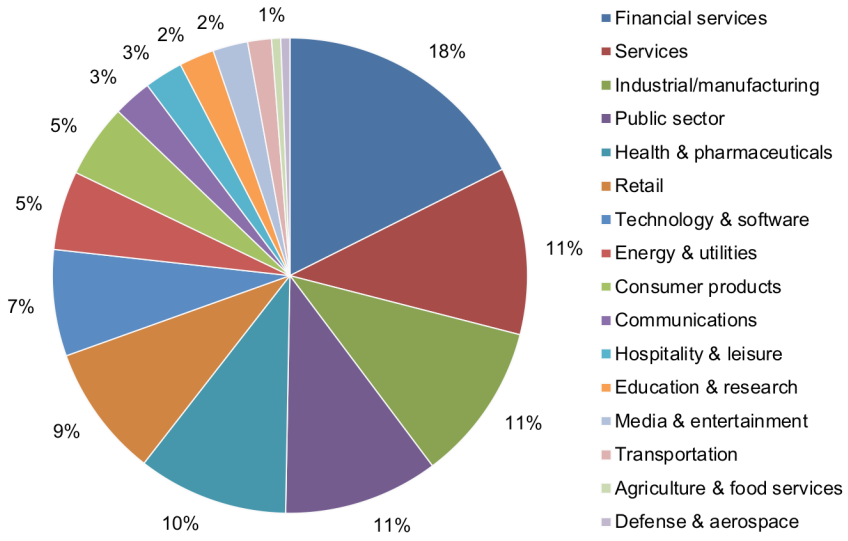
Methods

Methods

Table 1. Sample response	US	UK	Consolidated
Sampling frame	419	299	718
Total returns	146	97	243
Rejected or screened surveys	21	18	39
Final sample	125	77	202
Response rate	30%	26%	28%

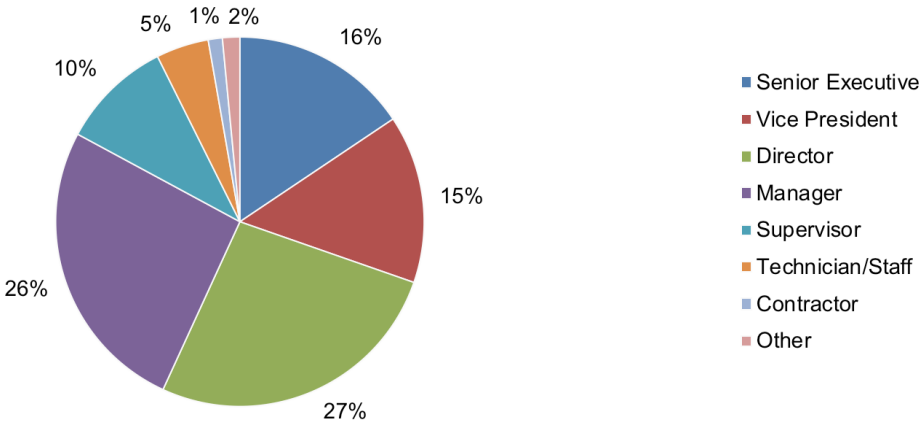
About the sample – The sample includes 202 senior-level IT and IT security practitioners in 16 verticals (68 percent hold the CISO title). A total of 125 are US-based multinational companies and 77 companies are located in the UK. The top 3 industries are as follows: (1) financial services, (2) services, and (3) industrial/manufacturing.

Pie Chart 1. Primary industry focus



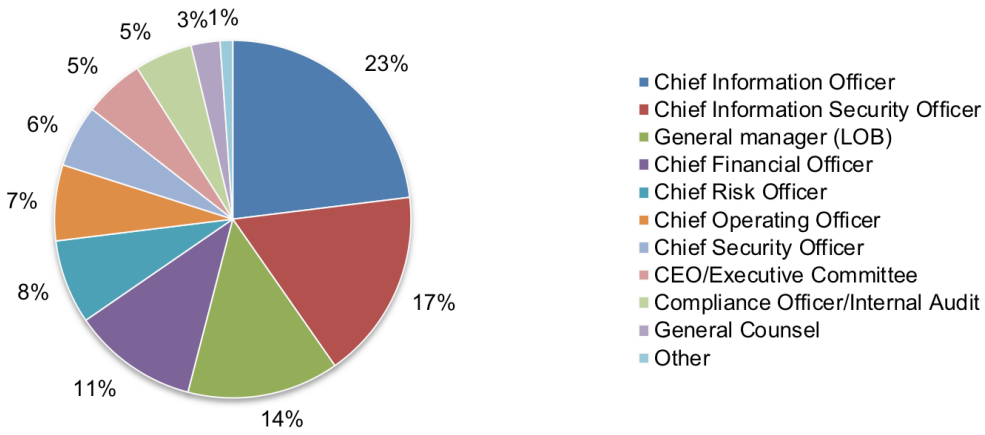
Pie Chart 1 reports the industry classification of the respondents' organizations. This chart identifies financial services (18 percent) as the largest segment, followed by services (11 percent), industrial/manufacturing (11 percent), and public sector (11 percent).

Pie Chart 2. Current position within the organization



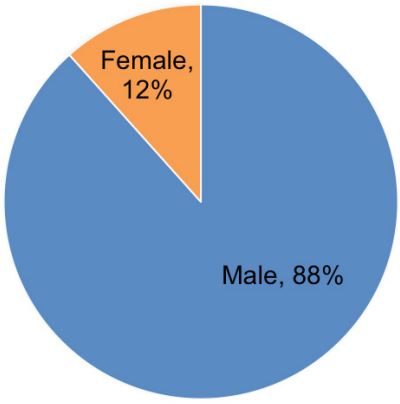
By design, 92 percent of respondents are either at or above the supervisory level, as shown in Pie Chart 2.

Pie Chart 3. Primary person reported to within the organization



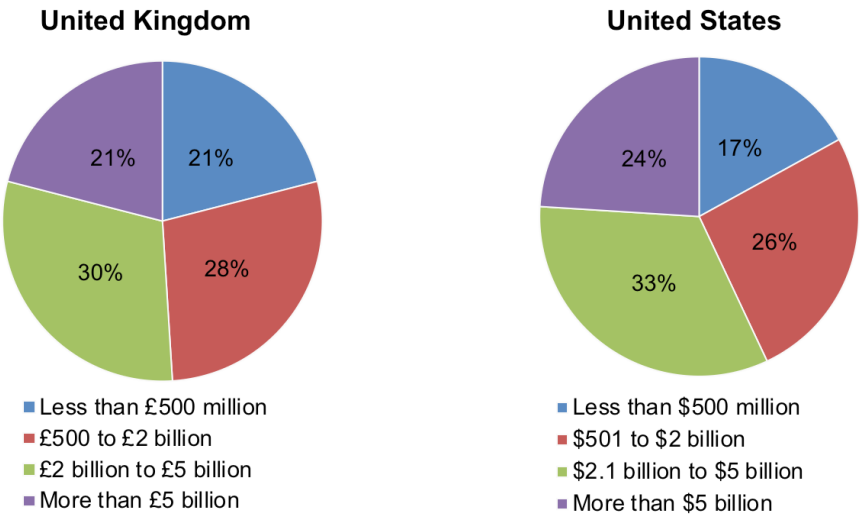
As shown in Pie Chart 3, 23 percent of respondents report to the chief information officer, 17 percent of respondents report to the chief information security officer and 14 percent of respondents report to the general manager (or line of business).

Pie Chart 4. Respondents' gender



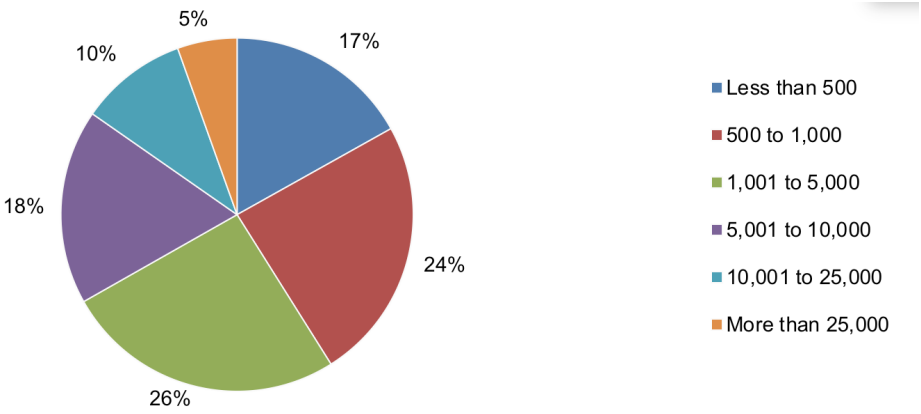
Eighty-eight percent of respondents are male and 12 percent of respondents are female, as shown in Pie Chart 4. Respondents reported having 10 years of IT or security experience and six years in their current position.

Pie Chart 5. Total annual revenue



Pie Chart 5 reports the organizations' total annual revenue for respondents in the United Kingdom and the United States. Fifty-one percent of respondents in the United Kingdom reported their organizations' annual revenue to be equal to or greater than £2 billion, and 57 percent of respondents in the United States reported their annual revenue to be equal to or greater than $2.1 billion.

Pie Chart 6. Global employee head count



Pie Chart 6 reveals that 59 percent of respondents are from organizations with a global head count of more than 1,000 employees.

PART 4

Appendix

- Caveats to this study
- Detailed survey results

CAVEATS TO THIS STUDY

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys:

- **Non-response bias:** The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.
- **Sampling-frame bias:** The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. We also acknowledge that the results may be biased by external events, such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.
- **Self-reported results:** The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

DETAILED SURVEY RESULTS

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured between September 14 and October 18, 2017.

Interview response	Consolidated
Total number of invitations	718
Total number of acceptances	243
Failed or rejected interviews	39
Final number of interviewees	202
Sample weights	1.00

Q1a. What best describes your level of knowledge about Vault 7?	Consolidated
Very familiar	23%
Familiar	35%
Somewhat familiar	25%
Not familiar	17%
No knowledge (stop)	0%
Total	100%

Q1b. What best describes your level of knowledge about ransomware attacks?	Consolidated
Very familiar	33%
Familiar	39%
Somewhat familiar	17%
Not familiar	11%
No knowledge (stop)	0%
Total	100%

Q2. Using the 10-point scale, please rate your level of knowledge about the following cybersecurity threats. 1 = no knowledge and 10 = detailed knowledge.

Q2a. Petya:	Consolidated
1 or 2 (no knowledge)	5%
3 or 4	13%
5 or 6	14%
7 or 8	26%
9 or 10 (detailed knowledge)	43%
Total	100%
Extrapolated value	7.25

Q2b. WannaCry:	Consolidated
1 or 2 (no knowledge)	3%
3 or 4	9%
5 or 6	18%
7 or 8	24%
9 or 10 (detailed knowledge)	45%
Total	100%
Extrapolated value	7.49

Q3. Using the 10-point scale, please rate your level of knowledge about the following Vault 7 components. 1 = no knowledge and 10 = detailed knowledge.

Q3a. Year Zero:	Consolidated
1 or 2 (no knowledge)	12%
3 or 4	26%
5 or 6	31%
7 or 8	13%
9 or 10 (detailed knowledge)	17%
Total	100%

Extrapolated value	5.44

Q3b. Dark Matter:	Consolidated
1 or 2 (no knowledge)	17%
3 or 4	30%
5 or 6	35%
7 or 8	12%
9 or 10 (detailed knowledge)	6%
Total	100%
Extrapolated value	4.66

Q3c. Grasshopper:	Consolidated
1 or 2 (no knowledge)	20%
3 or 4	32%
5 or 6	38%
7 or 8	7%
9 or 10 (detailed knowledge)	3%
Total	100%
Extrapolated value	4.36

Q3d. HIVE:	Consolidated
1 or 2 (no knowledge)	24%
3 or 4	34%
5 or 6	32%
7 or 8	7%
9 or 10 (detailed knowledge)	3%
Total	100%
Extrapolated value	4.15

Q3e. Weeping Angel:	Consolidated

1 or 2 (no knowledge)	25%
3 or 4	34%
5 or 6	30%
7 or 8	9%
9 or 10 (detailed knowledge)	2%
Total	100%
Extrapolated value	4.10

Q3f. After Midnight:	Consolidated
1 or 2 (no knowledge)	21%
3 or 4	38%
5 or 6	30%
7 or 8	8%
9 or 10 (detailed knowledge)	3%
Total	100%
Extrapolated value	4.17

Q4. Using the 10-point scale, please rate the risk level to your organization for each one of the following cybersecurity threats. 1 = low risk and 10 = substantial risk.

Q4a. Petya:	Consolidated
1 or 2 (low risk)	7%
3 or 4	8%
5 or 6	10%
7 or 8	25%
9 or 10 (substantial risk)	51%
Total	100%

Extrapolated value	7.62

Q4b. WannaCry:	Consolidated
1 or 2 (low risk)	7%
3 or 4	8%
5 or 6	13%
7 or 8	22%
9 or 10 (substantial risk)	51%
Total	100%
Extrapolated value	7.55

Q5. Using the 10-point scale, please rate the risk level to your organization for each one of the following Vault 7 components. 1 = low risk and 10 = substantial risk.

Q5a. Year Zero:	Consolidated
1 or 2 (low risk)	13%
3 or 4	11%
5 or 6	24%
7 or 8	23%
9 or 10 (substantial risk)	28%
Total	100%
Extrapolated value	6.35

Q5b. Dark Matter:	Consolidated
1 or 2 (low risk)	11%
3 or 4	15%
5 or 6	23%
7 or 8	25%
9 or 10 (substantial risk)	26%
Total	100%
Extrapolated value	6.31

Q5c. Grasshopper:	Consolidated
1 or 2 (low risk)	13%
3 or 4	16%
5 or 6	22%
7 or 8	25%
9 or 10 (substantial risk)	24%
Total	100%
Extrapolated value	6.13

Q5d. HIVE:	Consolidated
1 or 2 (low risk)	15%
3 or 4	17%
5 or 6	25%
7 or 8	24%
9 or 10 (substantial risk)	20%
Total	100%
Extrapolated value	5.85

Q5e. Weeping Angel:	Consolidated
1 or 2 (low risk)	9%
3 or 4	10%
5 or 6	28%
7 or 8	28%
9 or 10 (substantial risk)	24%
Total	100%
Extrapolated value	6.44

Q5f. After Midnight:	Consolidated
1 or 2 (low risk)	15%
3 or 4	15%
5 or 6	24%
7 or 8	26%
9 or 10 (substantial risk)	21%
Total	100%
Extrapolated value	5.98

Q6. Using the 10-point scale, please rate your organization's ability to prevent each one of the following cybersecurity threats. 1 = incapable and 10 = highly capable.

Q6a. Petya:	Consolidated
1 or 2 (incapable)	21%
3 or 4	19%
5 or 6	30%
7 or 8	16%
9 or 10 (highly capable)	13%
Total	100%
Extrapolated value	5.10

Q6b. WannaCry:	Consolidated
1 or 2 (incapable)	20%
3 or 4	20%
5 or 6	32%
7 or 8	14%
9 or 10 (highly capable)	14%
Total	100%

Extrapolated value	5.13

Q7. Using the 10-point scale, please rate your organization's ability to prevent each one of the following Vault 7 components. 1 = incapable and 10 = highly capable.

Q7a. Year Zero:	Consolidated
1 or 2 (incapable)	29%
3 or 4	27%
5 or 6	33%
7 or 8	8%
9 or 10 (highly capable)	2%
Total	100%
Extrapolated value	4.03

Q7b. Dark Matter:	Consolidated
1 or 2 (incapable)	36%
3 or 4	29%
5 or 6	26%
7 or 8	7%
9 or 10 (highly capable)	2%
Total	100%
Extrapolated value	3.74

Q7c. Grasshopper:	Consolidated
1 or 2 (incapable)	36%
3 or 4	29%
5 or 6	24%
7 or 8	6%
9 or 10 (highly capable)	5%
Total	100%

Extrapolated value	3.78

Q7d. HIVE:	Consolidated
1 or 2 (incapable)	37%
3 or 4	27%
5 or 6	26%
7 or 8	7%
9 or 10 (highly capable)	3%
Total	100%
Extrapolated value	3.71

Q7e. Weeping Angel:	Consolidated
1 or 2 (incapable)	37%
3 or 4	35%
5 or 6	15%
7 or 8	9%
9 or 10 (highly capable)	3%
Total	100%
Extrapolated value	3.62

Q7f. After Midnight:	Consolidated
1 or 2 (incapable)	35%
3 or 4	35%
5 or 6	20%
7 or 8	6%
9 or 10 (highly capable)	3%
Total	100%
Extrapolated value	3.64

Q8. Using the 10-point scale, please rate your organization's ability to detect each one of the following cybersecurity threats. 1 = incapable and 10 = highly capable.	
Q8a. Petya:	Consolidated
1 or 2 (incapable)	4%
3 or 4	12%
5 or 6	17%
7 or 8	31%
9 or 10 (highly capable)	36%
Total	100%
Extrapolated value	7.19

Q8b. WannaCry:	Consolidated
1 or 2 (incapable)	4%
3 or 4	10%
5 or 6	14%
7 or 8	32%
9 or 10 (highly capable)	40%
Total	100%
Extrapolated value	7.37

Q9. Using the 10-point scale, please rate your organization's ability to detect each one of the following Vault 7 components. 1 = incapable and 10 = highly capable.	
Q9a. Year Zero:	Consolidated
1 or 2 (incapable)	8%
3 or 4	15%
5 or 6	21%
7 or 8	26%
9 or 10 (highly capable)	30%

Total	100%
Extrapolated value	6.59

Q9b. Dark Matter:	Consolidated
1 or 2 (incapable)	12%
3 or 4	20%
5 or 6	21%
7 or 8	26%
9 or 10 (highly capable)	21%
Total	100%
Extrapolated value	5.98

Q9c. Grasshopper:	Consolidated
1 or 2 (incapable)	13%
3 or 4	22%
5 or 6	26%
7 or 8	22%
9 or 10 (highly capable)	17%
Total	100%
Extrapolated value	5.70

Q9d. HIVE:	Consolidated
1 or 2 (incapable)	10%
3 or 4	21%
5 or 6	28%
7 or 8	24%
9 or 10 (highly capable)	16%
Total	100%
Extrapolated value	5.80

Q9e. Weeping Angel:	Consolidated
1 or 2 (incapable)	12%
3 or 4	25%
5 or 6	24%
7 or 8	24%
9 or 10 (highly capable)	14%
Total	100%
Extrapolated value	5.53

Q9f. After Midnight:	Consolidated
1 or 2 (incapable)	13%
3 or 4	21%
5 or 6	26%
7 or 8	24%
9 or 10 (highly capable)	16%
Total	100%
Extrapolated value	5.71

Q10a. Were you aware of the US-CERT alert on Petya (ransomware)?	Consolidated
Yes	52%
No	43%
Unsure	5%
Total	100%

Q10b. If yes, did your organization implement the patches and follow the advice it gave?	Consolidated
Yes	55%
No	39%
Unsure	6%

Total	100%

Q11a. Were you aware of the US-CERT alert on WannaCry (ransomware)?	Consolidated
Yes	41%
No	51%
Unsure	7%
Total	100%

Q11b. If yes, did your organization implement the patches and follow the advice it gave?	Consolidated
Yes	44%
No	51%
Unsure	4%
Total	100%

Q12. With respect to the above-mentioned cybersecurity threats, do you believe the risk level to your organization will increase, decrease or stay at the same over the next 12 months?	Consolidated
Significant increase in risk	17%
Increase in risk	36%
Stay at about the same risk level	33%
Decrease in risk	10%
Significant decrease in risk	4%
Total	100%

Q13. Do you believe that these above-mentioned cybersecurity threats are more or less dangerous to an organization based on its size?	Consolidated
The larger the organization, the greater the risk	33%
The smaller the organization, the greater the risk	28%
Organizational size has no bearing on degree of risk	39%
Total	100%

Q14. Do you believe that these cybersecurity threats are more or less dangerous to public sector (governmental) organizations than commercial companies?	Consolidated
Public sector organizations are more susceptible to the above-mentioned cybersecurity threats	30%
Commercial organizations are more susceptible to the above-mentioned cybersecurity threats	37%
Public sector and commercial organizations are equally susceptible	32%
Total	100%

Q15. Do you believe that these cybersecurity threats are more or less dangerous based on the organization's geographic footprint?	Consolidated
Organizations with a global footprint are more susceptible to the above cybersecurity threats	46%
Organizations with a regional footprint are more susceptible to the above cybersecurity threats	12%
Organizations with a domestic footprint are more susceptible to the above cybersecurity threats	13%
Geographic footprint has no bearing on degree of cybersecurity risk	28%
Total	100%

Q16a. Have any of the above-mentioned cybersecurity threats been detected on your organization's network?	Consolidated
Yes	54%
No	37%
Unsure	9%
Total	100%

Q16b. If yes, which cybersecurity threats were detected? Please check all that apply.	Consolidated
WannaCry	25%
Petya	20%
Year Zero	9%
Dark Matter	15%
Grasshopper	15%
HIVE	20%

Weeping Angel	34%
After Midnight	31%
Total	170%

Q16c. For each one of the above-mentioned threats that were detected, was your organization able to resist the attack?	Consolidated
Yes	48%
No	47%
Unsure	5%
Total	100%

Q16d. For the above-mentioned threats that were detected, what was the consequence of the attack? Please check all that apply.	Consolidated
Exfiltration (theft) of data assets	52%
Disruption to IT operations (downtime)	41%
Disruption to business process	47%
Damage to IT infrastructure	21%
Loss revenues	14%
None of the above	35%
Other (please specify)	3%
Total	212%

Q16e-1. For the above-mentioned threats that were detected, which amount (range) best describes economic damages to your organization?	UK
None	2%
Less than £1,000	4%
£1,001 to £10,000	3%
£10,001 to £50,000	9%
£50,001 to £100,000	14%
£100,001 to £500,000	20%
£500,001 to £1,000,000	36%
£1,000,001 to £10,000,000	10%
More than £10,000,000	2%
Total	100%
Extrapolated value	£1,113,401

Q16e-1. For the above-mentioned threats that were detected, which amount (range) best describes economic damages to your organization?	US
None	0%
Less than $1,000	1%
$1,001 to $10,000	4%
$10,001 to $50,000	4%
$50,001 to $100,000	7%
$100,001 to $500,000	23%
$500,001 to $1,000,000	38%
$1,000,001 to $10,000,000	15%
More than $10,000,000	8%
Total	100%
Extrapolated value	$2,065,679

Q17. What cyberattacker (hacker) presents the greatest risk to your organization?	Consolidated

Lone wolf (individual) hacker	11%
Organized hacking group or syndicate	42%
Hacktivist	17%
Nation-state attackers	26%
Other (please specify)	5%
Total	100%

Q18. Does your organization have personnel (specialists) who have the expertise to tackle the above-mentioned cybersecurity threats?	Consolidated
Yes, internal resources	25%
Yes, external resources (MSP/MSSP)	17%
Yes, mixture of internal and external resources	24%
No	33%
Total	100%

Q19. Are your organization's enabling security technologies sufficient for preventing, detecting and containing the above-mentioned cybersecurity threats?	Consolidated
Yes	45%
No	40%
Unsure	14%
Total	100%

Q20a. Is your organization's IT security budget ample for preventing, detecting and containing the above-mentioned cybersecurity threats?	Consolidated
Yes	47%
No	48%
Unsure	4%
Total	100%

Q20b. If yes, do you believe your organization's IT security budget will need to increase to tackle the above-mentioned cybersecurity threats?	Consolidated
Yes, significant increase	25%
Yes, some increase	60%
No	9%
Unsure	7%
Total	100%

Q20c-1. If yes, will your organization's budget increase focus on internal activities or on external support (e.g., managed security service provider)?	Consolidated
Spending mostly on internal activities	33%
Spending mostly on external services	27%
Spending on both internal activities and external services	40%
Total	100%

Q20c-2. [If external] Is your current MSSP/MSP able to prevent, detect and/or contain the above-mentioned cybersecurity threats?	Consolidated
Yes	45%
No	44%
Unsure	11%
Total	100%

Demographics and organizational characteristics

D1. What organizational level best describes your current position?	Consolidated
Senior Executive	16%
Vice President	15%
Director	27%
Manager	26%
Supervisor	10%
Technician/Staff	5%
Contractor	1%
Other	2%
Total	100%

D2. Check the Primary Person you or your manager reports to within the organization.	Consolidated
CEO/Executive Committee	5%
Chief Operating Officer	7%
Chief Financial Officer	11%
General Counsel	3%
General Manager (LOB)	14%
Chief Information Officer	23%
Chief Information Security Officer	17%
Chief Security Officer	6%
Compliance Officer/Internal Audit	5%
Chief Risk Officer	8%
Other	1%
Total	100%

D3. Total years of relevant experience	Consolidated
Total years of IT or security experience	10.42

Total years in current position	6.33

D4. Gender:	Consolidated
Female	12%
Male	88%
Total	100%

D5. What industry best describes your organization's industry focus?	Consolidated
Agriculture & food services	1%
Communications	3%
Consumer products	5%
Defense & aerospace	1%
Education & research	2%
Energy & utilities	5%
Financial services	18%
Health & pharmaceuticals	10%
Hospitality & leisure	3%
Industrial/manufacturing	11%
Media & entertainment	2%
Public sector	11%
Retail	9%
Services	11%
Technology & software	7%
Transportation	2%
Total	100%

D6a. What best defines the total annual revenue of your organization (to be translated into local current):	UK
Less than £500 million	21%
£500 to £2 billion	28%
£2 billion to £5 billion	30%
More than £5 billion	21%
Total	100%

D6b. What best defines the total annual revenue of your organization (to be translated into local current)?	US
Less than $500 million	17%
$501 to $2 billion	26%
$2.1 billion to $5 billion	33%
More than $5 billion	24%
Total	100%

D7. What is the worldwide headcount of your organization?	Consolidated
Less than 500	17%
500 to 1,000	24%
1,001 to 5,000	26%
5,001 to 10,000	18%
10,001 to 25,000	10%
More than 25,000	5%
Total	100%
Extrapolated value	5,728

Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.

PONEMON INSTITUTE

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the Council of American Survey Research Organizations (CASRO), we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.