Measuring & Managing the Cyber Risks to Business Operations

SPONSORED BY TENABLE

Independently conducted by Ponemon Institute LLC

Publication Date: December 2018

Measuring & Managing the Cyber Risks to Business Operations

Ponemon Institute, December 2018

PART 1. EXECUTIVE SUMMARY

Measuring & Managing the Cyber Risks to Business Operations, which was sponsored by Tenable and conducted by Ponemon Institute, reveals global trends in how organizations are assessing and addressing cybersecurity risks. We conclude from the findings that current approaches to understanding cyber risks to business operations are failing to help organizations minimize and mitigate threats.

We surveyed 2,410 IT and IT security practitioners in the United States, United Kingdom, Germany, Australia, Mexico and Japan. All respondents have involvement in the evaluation and/or management of investments in cybersecurity solutions within their organizations. The consolidated global findings are presented in this report.

Following is a high-level summary of the findings

- **Cyber attacks are relentless and continuous**. Most organizations represented in this research are experiencing multiple cyber attacks causing data breaches as well as significant disruption and downtime to business operations, plant and operational equipment.

- **Reasons organizations continue to face serious security challenges.** According to the findings, following are the reasons organizations are vulnerable to cyber attacks: An understaffed IT security function; lack of resources to manage vulnerabilities; the proliferation of IoT devices in the workplace; complexity of the IT security infrastructure; lack of controls over third-party access to sensitive and confidential data; dependency on manual processes to respond to vulnerabilities; and insufficient visibility into their organization's attack surface.

- **New approaches for measuring cyber risks are needed.** Current and common cyber KPIs (see sidebar) are inadequate for three key reasons: 1) they focus on the tech side of the issue without fully considering the financial and business implications; 2) they are tactical, rather than strategic, in nature and 3) they reflect the widespread inability to effectively prioritize risk. Put another way, they fall far short of reflecting digital business and digital transformation.

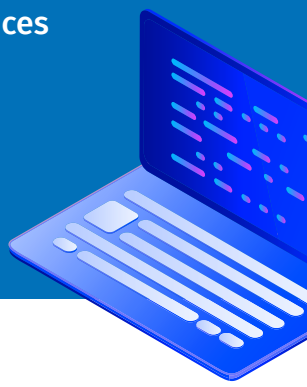
- **We don't know what we don't know.** Organizations are not accurately measuring the business costs of cyber risk, and are unable to quantify the damage cyber attacks could have on their businesses. Thus, decisions about the allocation of resources, investments in technologies and the prioritization of threats are being made without critical information.

KPIs Used to Measure Cyber Risk

- Time to assess cyber risk
- Time to remediate cyber risk
- Identification of OT & IoT assets vulnerable to cyber risk
- Effectiveness in prioritizing cyber risks

KPIs Used to Measure Financial Consequences

- Loss of revenue
- Loss of productivity
- Drop in stock price



- **Boards of directors are in the dark about the true cost of cyber risks to their organizations.** Without confidence in the accuracy of their measures, CISOs and other security executives are reluctant to share critical information with their boards about the business costs of cyber risks.

PART 2. KEY FINDINGS

In this section, we analyze the findings of research. The complete audited findings are presented in the Appendix of this report. We have organized the findings according to the following topics.

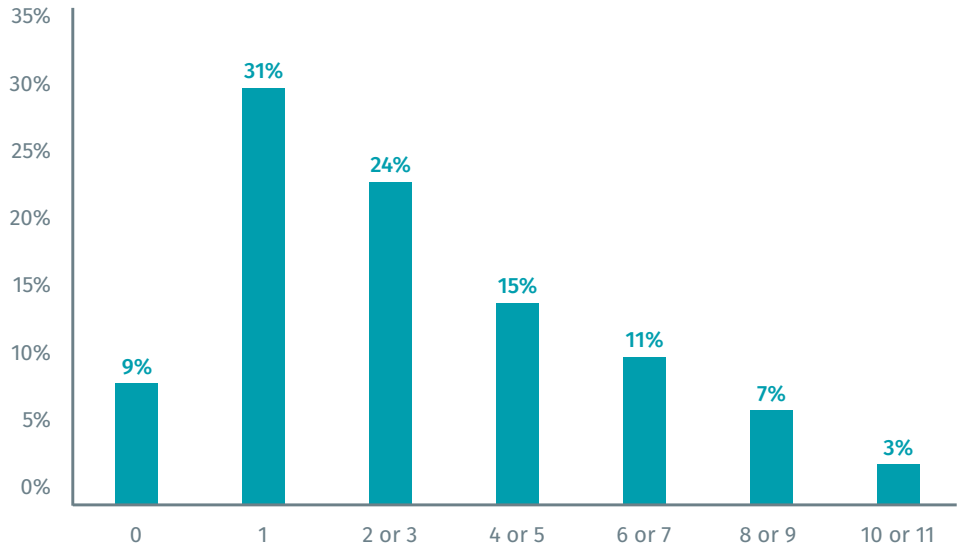
- Why organizations are experiencing multiple business-disrupting cyber attacks
- Measurements used to assess cyber risks to business operations
- Priorities for measuring and managing cyber risks
- Current approaches to vulnerability and cyber risk management
- Country differences
- Five recommendations for improving the ability to mitigate cyber risks

Why organizations are experiencing multiple business-disrupting attacks

Cyber attacks are relentless and continuous. As shown in Figure 1, 91 percent of organizations represented in this study have experienced at least one damaging cyber attack over the past two years and 60 percent have had two or more. These attacks have resulted in data breaches and/or significant disruption and downtime to business operations, plants and operational equipment. The list of cyber attacks experienced by organizations is presented in Figure 2.

Figure 1. Organizations are experiencing multiple damaging cyber attacks

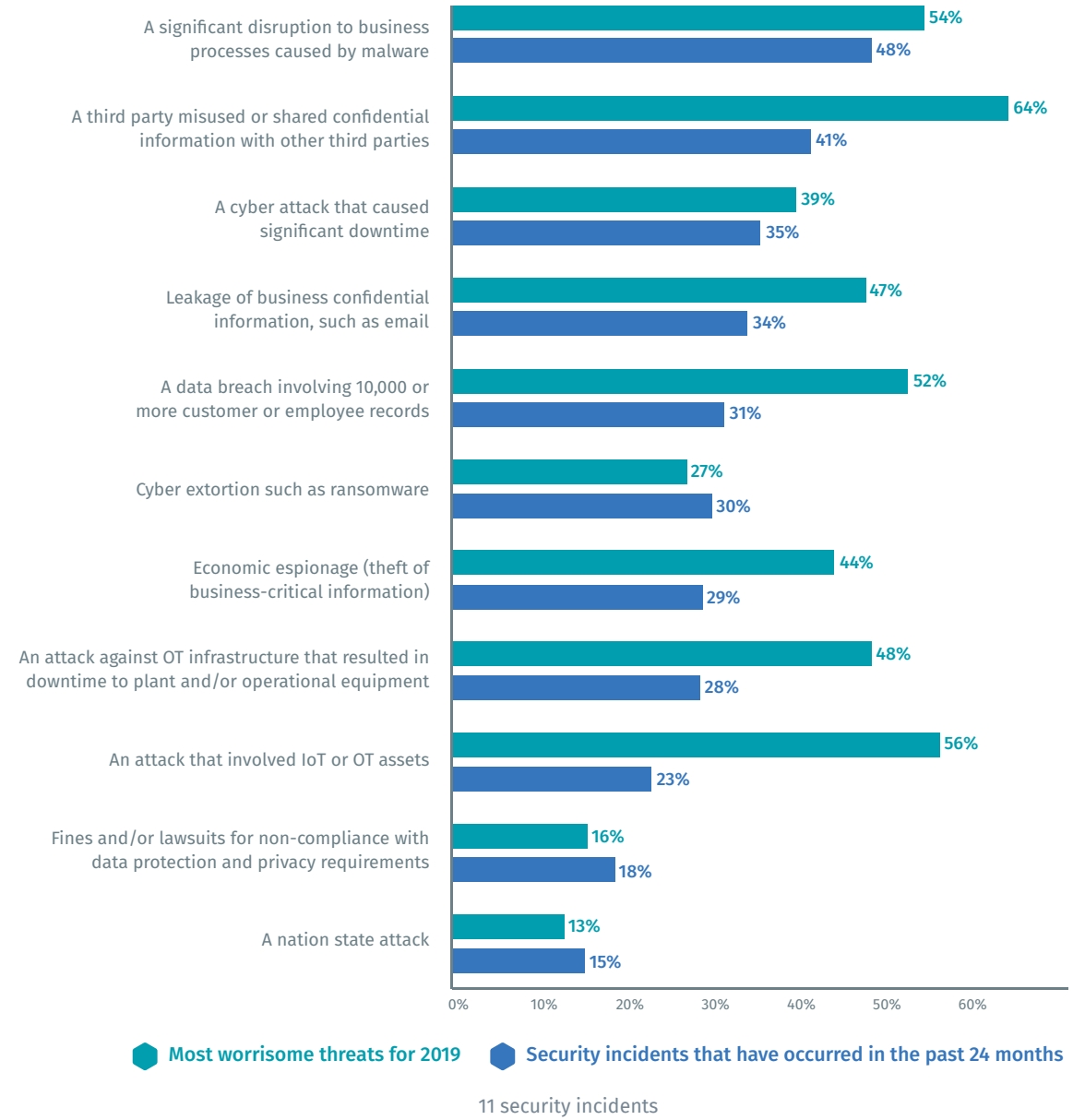
Number of cyber attacks experienced over the past 24 months



The highest-rated cybersecurity concerns for 2019 are third-party risks, data breaches and attacks on IoT or Operational Technology (OT) assets. Respondents were asked if their organization experienced any of 11 different security incidents, as shown in Figure 2, and to project which security incidents they are most concerned about in 2019. The teal bar shows the most worrisome threats for 2019 and the blue bar indicates the cyber attacks experienced. Forty-eight percent of respondents say their organization experienced a significant disruption to business processes caused by malware and 41 percent of respondents say a third party misused or shared confidential information with other third parties. Both of these security incidents are expected to increase in frequency in 2019.

While less than a quarter of respondents (23 percent) say their organizations experienced an attack involving IoT or OT assets in the past two years, more than half (56 percent of respondents) say it's something they're most worried about in 2019. Additionally, more than half (52 percent of respondents) say they are concerned about a data breach involving 10,000 or more customer or employee records in 2019.

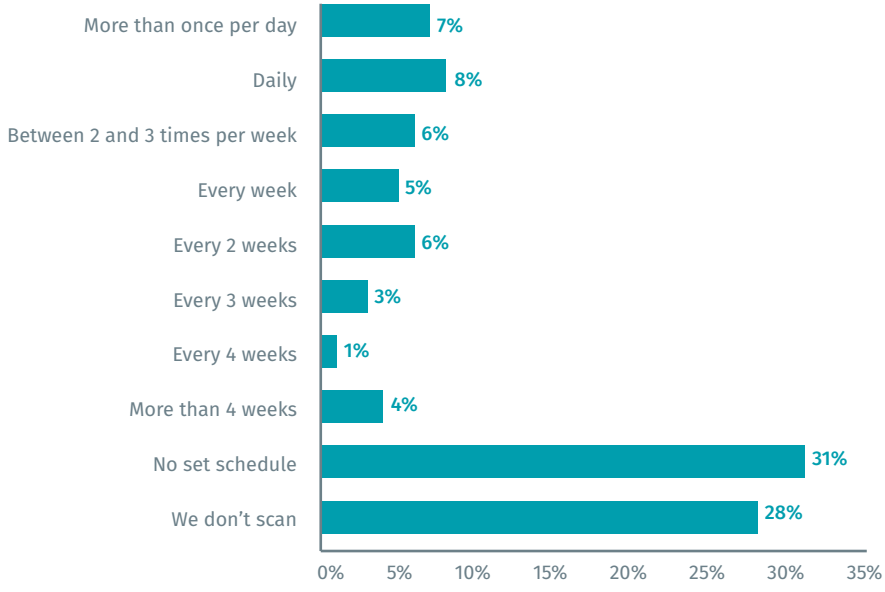
Figure 2. Security incidents most worrisome for 2019 and the cyber attacks organizations have experienced



Most respondents say their IT security function is understaffed to scan for vulnerabilities in a timely manner. Organizations represented in this research have an average of 19 employees involved in vulnerability management. However, the majority of respondents (58 percent) say the security function does not have adequate staffing to scan vulnerabilities in a timely manner. Shortages in skilled staff affect the ability to scan for publicly disclosed vulnerabilities. As shown in Figure 3, 59 percent say their organizations have no set schedule to scan (31 percent) or do not scan (28 percent).

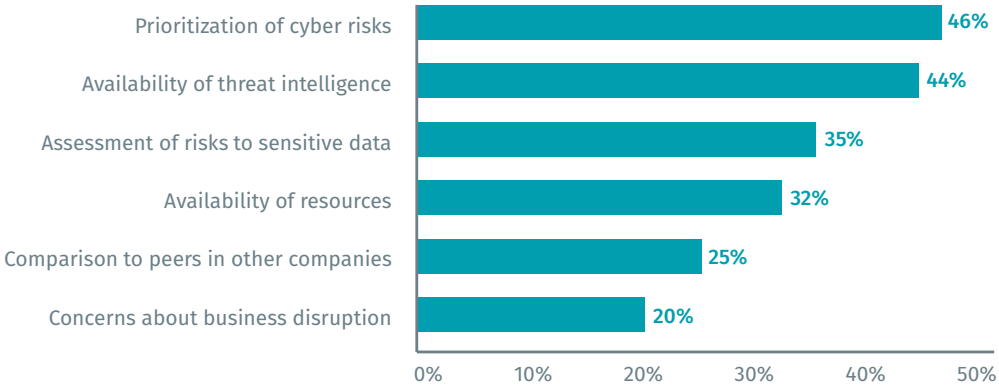
Figure 3.
How quickly does your organization scan for vulnerabilities once they have been publicly disclosed?

59%
of respondents have no set schedule or don't scan (31 percent + 28 percent)



The frequency of scanning for vulnerabilities is determined by the organization's ability to prioritize cyber risks. The scanning behavior of organizations is often an indicator of cyber maturity; mature organizations tend to prioritize their scan frequency based on the level of cyber risks and the level of risk to sensitive data. As shown in Figure 4, 46 percent of respondents say prioritization of cyber risks is a factor in their scan frequency decisions. Yet, just 35 percent of respondents say scanning is determined by an assessment of risks to sensitive data.

Figure 4. What determines the frequency of scanning?



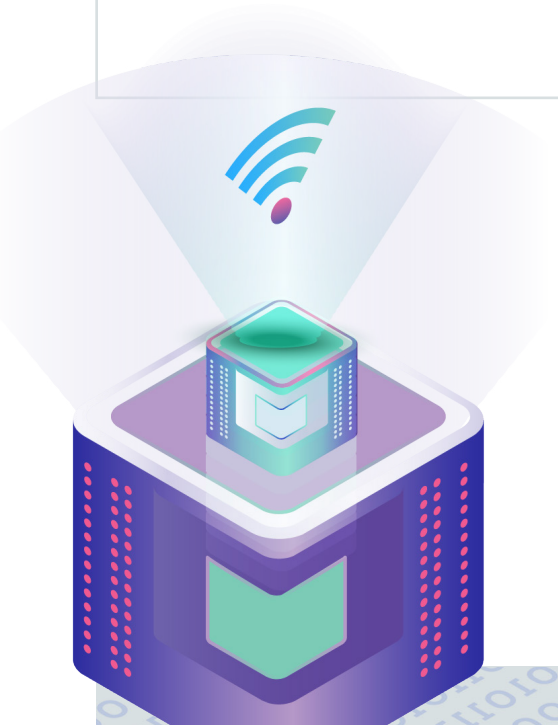
More than one response permitted

Reliance upon manual processes is a barrier to reducing vulnerabilities. It's not uncommon for organizations to rely on an assortment of spreadsheets to track assets and vulnerabilities, relying on staff to identify and resolve issues by hand, slowing teams down. More than half of respondents (51 percent) say their security teams spend more time navigating manual processes than responding to vulnerabilities, leading to insurmountable response backlogs (see Figure 5). Almost half of respondents (48 percent) say their organizations are at a disadvantage in responding to vulnerabilities due to the use of manual processes.

As will be discussed later in the report, 80 percent of respondents say threat intelligence is very important to setting their cybersecurity priorities. However, only 39 percent of respondents say they are incorporating threat intelligence when prioritizing which assets are most important to safeguard. Organizations' vulnerability management programs are also at a disadvantage because only 29 percent of respondent say they have sufficient visibility into their complete attack surface (i.e. cloud, containers, IoT and OT).

Figure 5. Perceptions about responding to vulnerabilities and threats

Strongly agree and agree responses combined

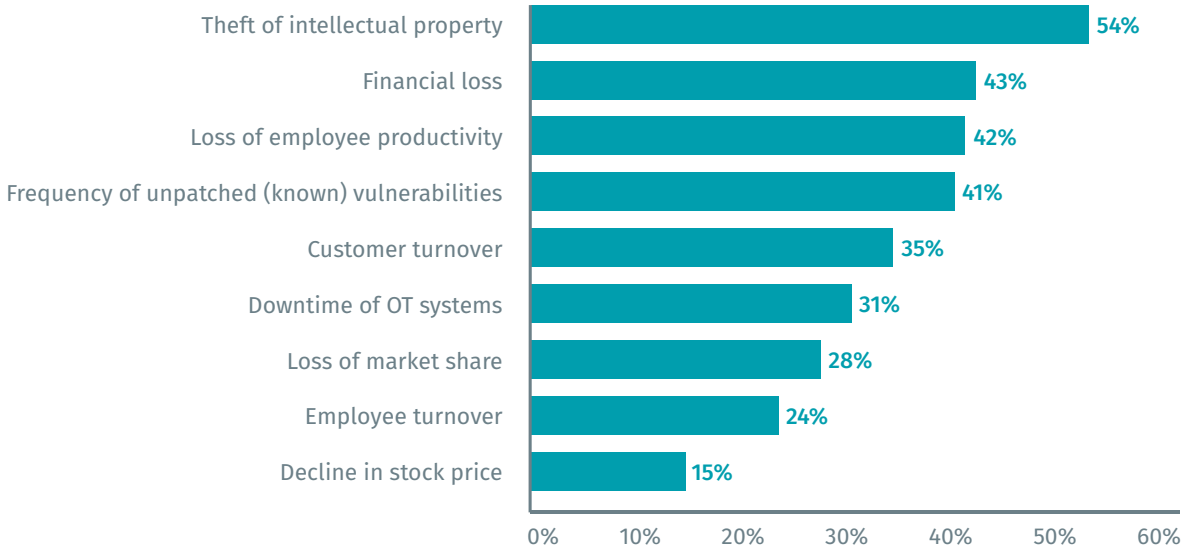


Most organizations are not quantifying what a security incident would cost their organizations. Only 41 percent of respondents say their organizations attempt to quantify the damage the 11 incidents listed in Figure 2 could have on their businesses. The factors these organizations use to quantify the risk are listed in Figure 6. Of the 988 respondents who say their organizations attempt to quantify security incidents:

- 54 percent say they quantify what the theft of intellectual property would cost;
- 43 percent say they calculate the potential financial loss; and
- 42 percent consider the impact of the loss of employee productivity following a data breach or security exploit.

While conventional wisdom suggests a decline in stock price would be a major consideration in quantifying the risk of a cyber attack, only 15 percent of respondents cite this as a factor. However, when we filter this response to show only those who work for publicly traded companies (1,163 or 48 percent of respondents), we see a change. Nearly one-third of respondents working in publicly traded companies (31 percent) say they use a decline in stock price as a factor.

Figure 6. What factors are used to quantify the potential risk of a cyber attack?



More than one response permitted

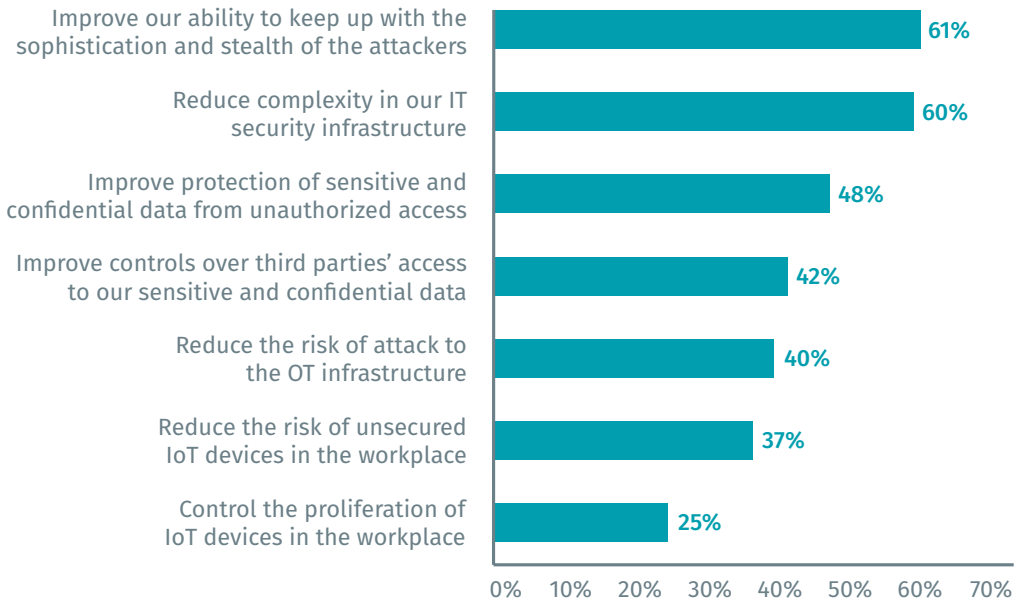
To help mitigate cyber attacks, new approaches for measuring cyber risks are needed. As shown in Figure 7, traditional KPIs or metrics for evaluating business risks cannot be used to understand cyber risks. Further, only 30 percent of respondents say they agree their organizations are able to correlate information from cyber risk KPIs to taking action on reducing the risk of a data breach or security exploit.

Figure 7. Perceptions about KPIs

Strongly agree and agree responses combined

Keeping ahead of attackers and reducing complexity in the IT security infrastructure are two priorities for 2019. Figure 8 lists the risks organizations need to address in order to improve their security posture. Sixty-one percent of respondents say their goal is to improve the ability to keep up with the sophistication and stealth of the attackers and 60 percent say reducing complexity is important.

Figure 8. The top seven security priorities for 2019



More than one response permitted

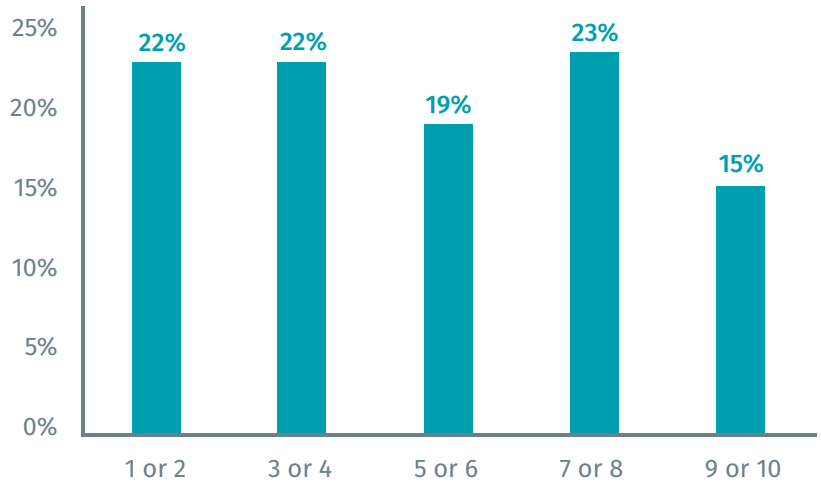
Measurements used to assess cyber risks to business operations

Most organizations are not measuring the business costs of cyber risk. Less than half of respondents (46 percent or 1,109) measure and, therefore, understand what cyber risks are costing their organizations. Of these 1,109 respondents, only 41 percent say they are required to report the results of such analysis to the board of directors.

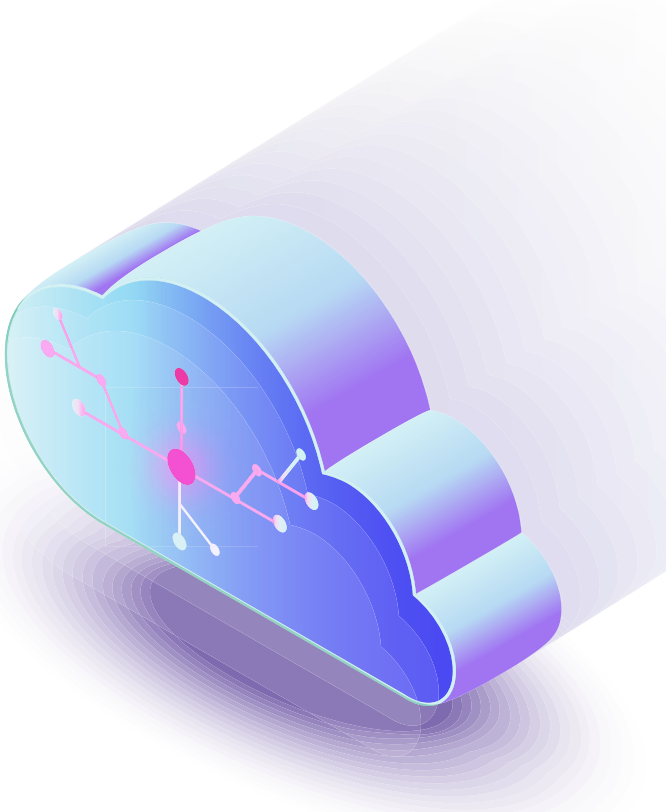
We asked respondents to rate the accuracy of the information measured on a scale of 1 = not accurate to 10 = very accurate.

Figure 9.
How accurate is your organization in measuring the business costs of cyber risk?

On a scale of 1 = not accurate to 10 = very accurate



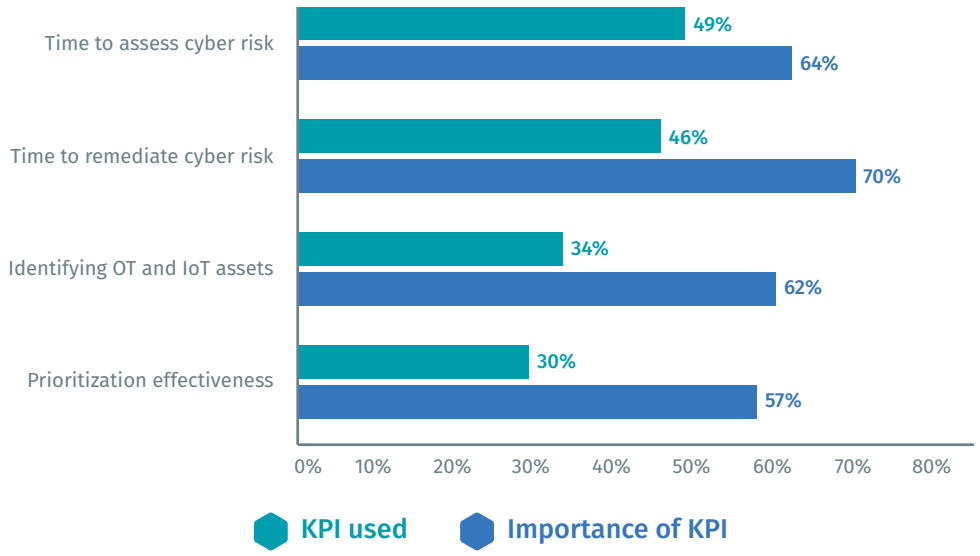
Only
38%
of respondents believe their measures are very accurate
(23 percent + 15 percent)



Organizations are not using the KPIs they consider most important to assessing and understanding cyber threats. Respondents were asked if their organizations are using the KPIs listed in Figure 10 and to rank how essential these KPIs are to minimizing cyber risk on a scale of 1 = not important to 10 = essential. As shown, there is a significant gap between the use of these KPIs and their perceived importance, especially with respect to identifying OT and IoT assets. Specifically, 34 percent of respondents say they use this KPI and 62 percent say it is essential.

Figure 10. Gap in the use and importance of KPIs

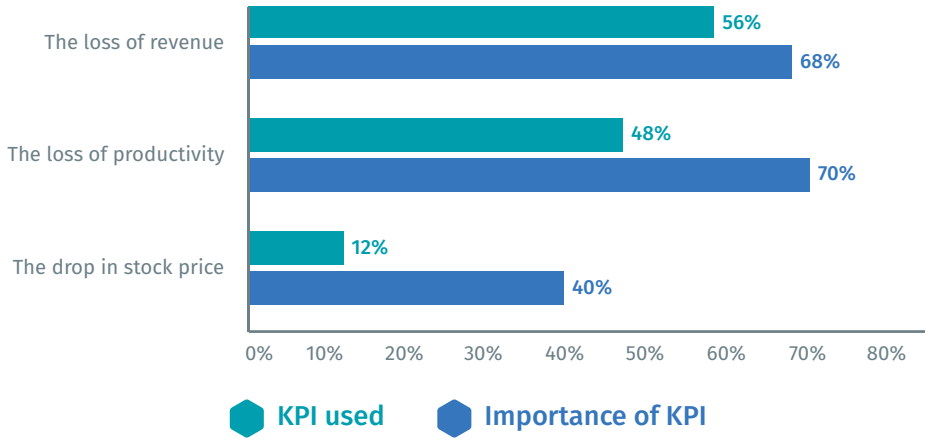
Yes responses and Very important and essential responses presented



Organizations are not using the KPIs they consider most important to measuring the business impact of a cyber attack. Respondents were asked if their organizations are using the KPIs listed in Figure 11 and to rank how essential these KPIs are to understanding the consequences of a cyber attack on a scale of 1 = not important to 10 = essential. As shown, there is a significant gap between the use of these KPIs and their perceived importance, especially with respect to measuring the decline in stock price. As we saw earlier in this report, only 15 percent of respondents cited a decline in stock price as a factor when considering cyber risk (Figure 6). In the answer set reflected in Figure 11, the question was phrased slightly differently; we asked respondents whether stock price is a KPI they actually use, and in this case only 12 percent of respondents said yes. Yet, four in 10 respondents (40 percent) identify stock price as an important KPI.

Figure 11. Gap in use and importance of non-security measures

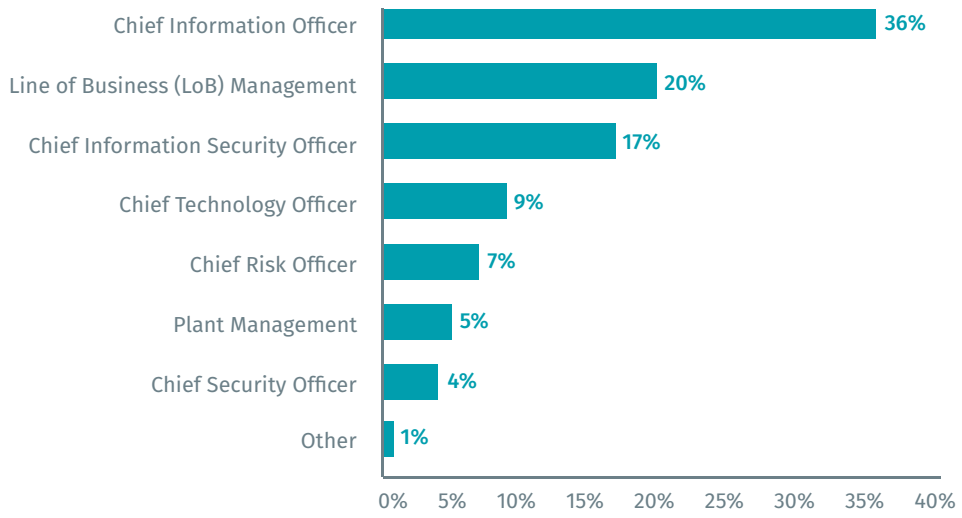
Yes responses and Very important and essential responses presented



Priorities for measuring and managing cyber risks

Responsibility for evaluating cyber risk is dispersed throughout the organization. As shown in Figure 12, responsibility for the evaluation of cyber risk as part of an organization's business risk management practice is dispersed throughout the organization. However, 66 percent of respondents say at least one of the following is involved in the evaluation of cyber risks: the CIO (36 percent); the CISO (17 percent); the CTO (9 percent); and the CSO (4 percent).

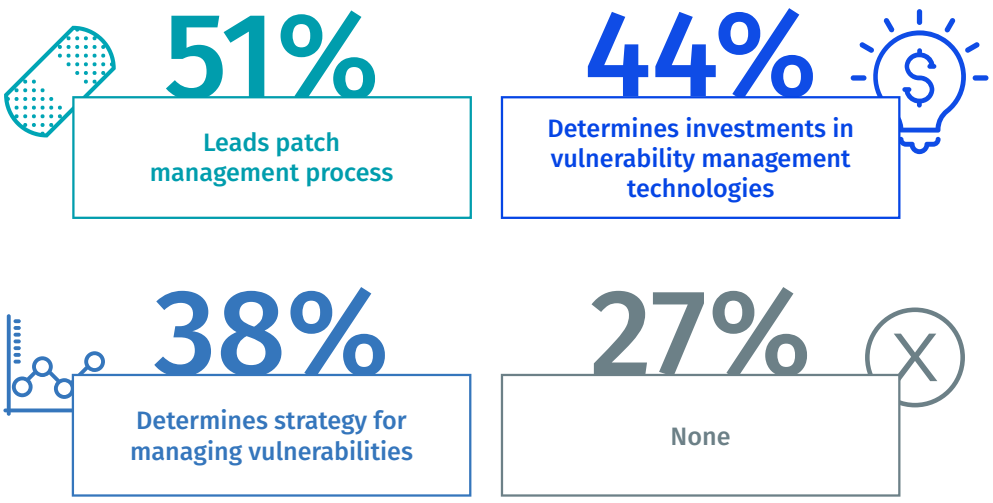
Figure 12.
Who is most involved in the evaluation of cyber risk as part of your organization's business risk management?



CISOs are leading the patch management process. Seventy-three percent of respondents say their CISOs or security leaders are involved in vulnerability management. As presented in Figure 13, 51 percent of respondents say their CISOs lead the patch management process and 44 percent of respondents say the CISO determines investments in vulnerability management. Only 38 percent of respondents say the CISO determines strategy for managing vulnerabilities.

Figure 13. What role does the CISO play in vulnerability management within your organization?

More than one response permitted



Many respondents say their organizations are very effective in prioritizing threats critical to business assets. Fifty-nine percent of respondents (1,421) say their organizations succeed at prioritizing threats that target critical business assets. Of these 1,421 respondents, 55 percent say they are effective because of their ability to quickly remediate security exploits and/or data breaches. Nearly half of these 1,421 respondents (47 percent) cite their organization's ability to quickly assess vulnerabilities as a reason why they're effective in prioritizing threats. Similarly, 46 percent of these respondents say they're effective in prioritizing threats because of their ability to assess vulnerabilities in all critical IT, OT and IoT assets, as shown in Figure 14.

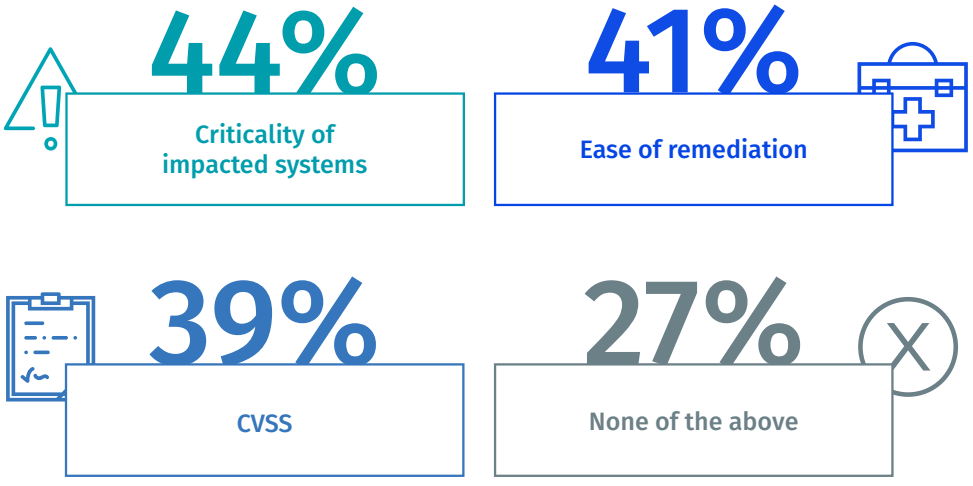
Figure 14. Why certain organizations are effective in prioritizing threats to critical business assets

More than one response permitted

There is a marked disconnect in how organizations prioritize threats. Respondents could select more than one choice to indicate how their organizations prioritize threats to critical business assets. As shown in Figure 15, 44 percent of respondents say their organizations consider how critical it would be if specific systems were impacted by a cyber attack, which we consider to be an indicator of a mature cybersecurity posture. At the same time, 41 percent of respondents also say they prioritize based on the ease of remediation, which we consider to be one of the least-mature approaches to prioritization.

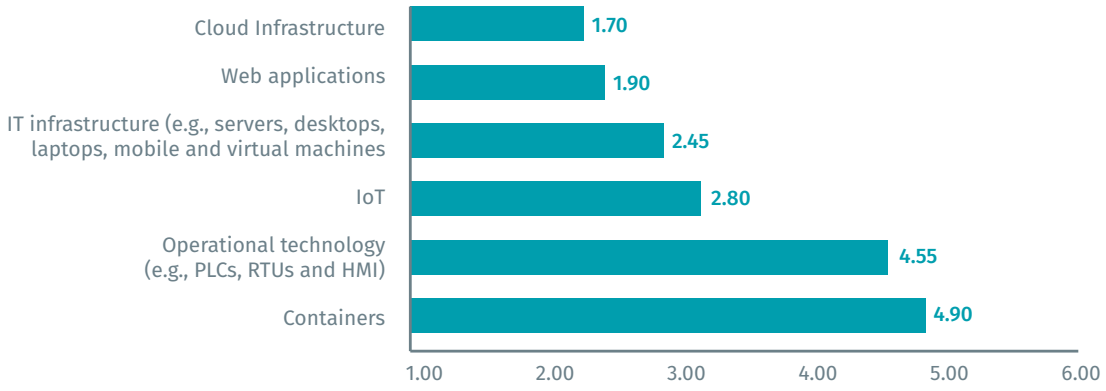
Figure 15.
How does your organization prioritize threats to critical business assets?

More than one response permitted



The cloud is considered the most important asset to safeguard. Respondents were asked to rank the asset types they believe are most important to safeguard, from 1 = highest priority to 6 = lowest priority. As shown in Figure 16, respondents are most focused on protecting their cloud infrastructure and web applications from cyber attacks.

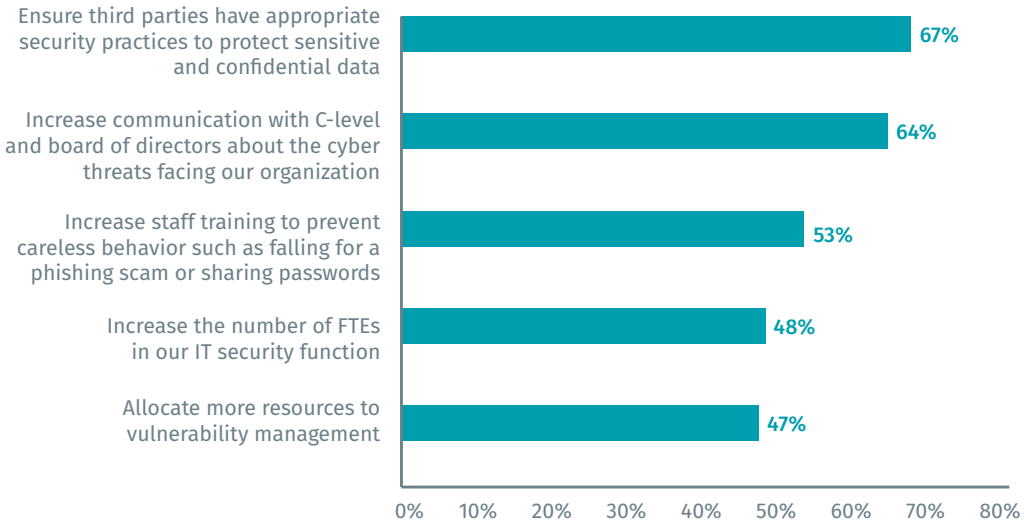
Figure 16. Priorities ranked for measuring and managing 2019 cyber risks



From 1 = highest priority to 6 = lowest priority

Reducing the third-party risk is the top governance priority for 2019. According to Figure 17, organizations will focus on ensuring that third parties have appropriate security practices to protect sensitive and confidential data followed by increasing communication with C-level and board of directors about the cyber threats facing their organizations.

Figure 17. The top 5 governance priorities for 2019



More than one response permitted

To prioritize cyber risks, threat and peer-to-peer intelligence sharing is essential. Respondents were asked to rate the importance of threat and peer-to-peer intelligence sharing on a scale of 1 = not important at all to 10 = essential. As shown in Figure 18, 80 percent of respondents say threat intelligence is very important and even essential and 67 percent of respondents say peer-to-peer intelligence sharing and collaboration is important for setting cybersecurity priorities.

Figure 18. Importance of threat and peer-to-peer intelligence sharing

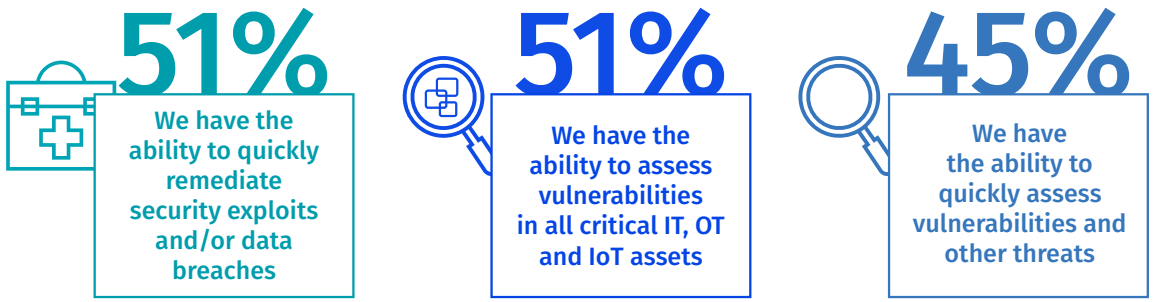
From 1 = not important at all to 10 = essential, 7+ responses presented

Current approaches to vulnerability and cyber risk management

The ability to quickly remediate security exploits and assess vulnerabilities are cited as reasons organizations are effective in minimizing the consequences of a cyber attack. Sixty percent of respondents say their organizations are effective in reducing the impact of a cyber attack on their business operations.

According to Figure 19, the primary reasons for their effectiveness are the ability to quickly remediate security exploits and/or data breaches and the ability to assess vulnerabilities in all critical IT, OT and IoT assets. Fewer respondents say their organization has the ability to quickly assess vulnerabilities and other threats (45 percent of respondents).

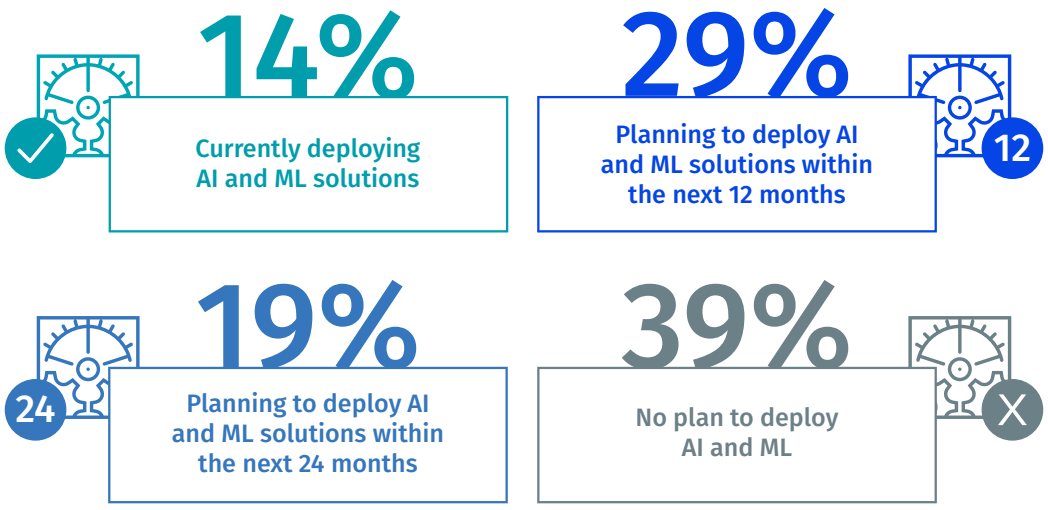
Figure 19. Why certain organizations believe they are effective in minimizing the success of a cyber attack?

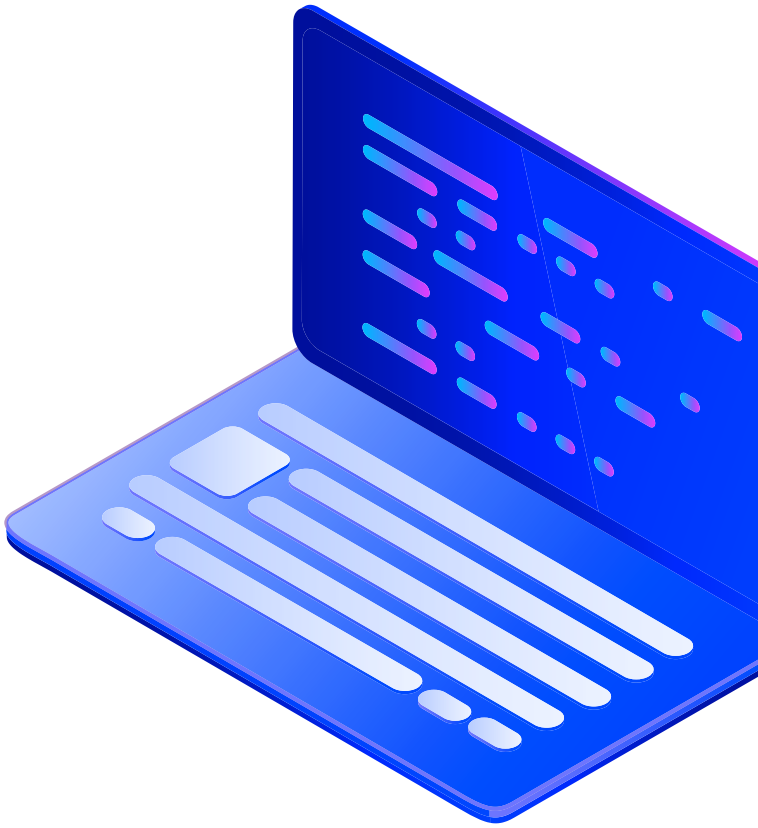


More than one response permitted

Most organizations have or plan to use artificial intelligence (AI) and machine learning (ML) for vulnerability management. According to Figure 20, 62 percent of respondents say they are currently deploying AI and ML solutions or plan to within the next two years.

Figure 20. Does your organization plan to use AI and ML for vulnerability management?





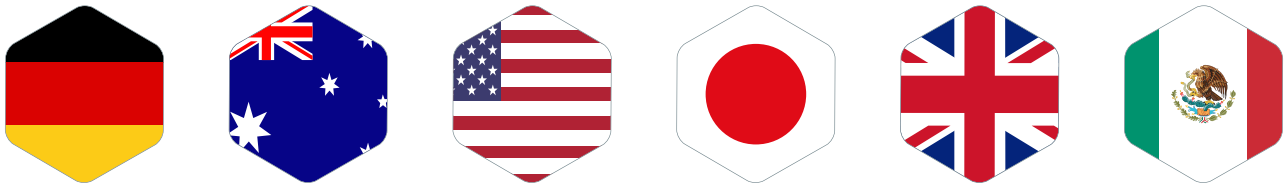
Country Differences

In this section, we present the most interesting differences among the countries represented in this research. The countries participating in this study are: United States (US), United Kingdom (UK), Germany (DE), Australia (AU), Mexico (MX) and Japan (JP). Following are five examples of how these countries' approaches to measuring and managing cyber risks are similar or vary significantly.

- With the exception of the UK and Mexico, approximately half of all countries represented are measuring the business costs of cyber risk. German respondents are most likely to believe the information from their metrics is accurate.
- All countries represented in this study believe in the importance of threat intelligence and peer-to-peer intelligence sharing.
- The use of non-security measures, such as loss of revenue and productivity, to understand the impact to business operations following a cyber attack varies significantly among countries. Specifically, 68 percent of respondents in Japan use this KPI. In contrast, less than half of German and Australian respondents say their organizations use this KPI (49 percent and 48 percent, respectively).
- The loss of productivity KPI is most likely to be used by UK organizations (56 percent of respondents) and least likely to be used by Japanese organizations (42 percent of respondents).
- Reliance upon manual processes is believed by many respondents to put their organizations at a disadvantage in responding to vulnerabilities. However, more Mexican respondents agree that their organizations are at disadvantage (55 percent). Respondents in UK organizations (55 percent) are more likely to agree that their security teams face insurmountable response backlogs because of time spent navigating manual processes.

German organizations are more likely to measure the business costs of cyber risk. According to Figure 21, 51 percent of German respondents measure the business costs of cyber risks. In contrast, 41 percent of respondents in Mexico and 42 percent of UK respondents measure these costs.

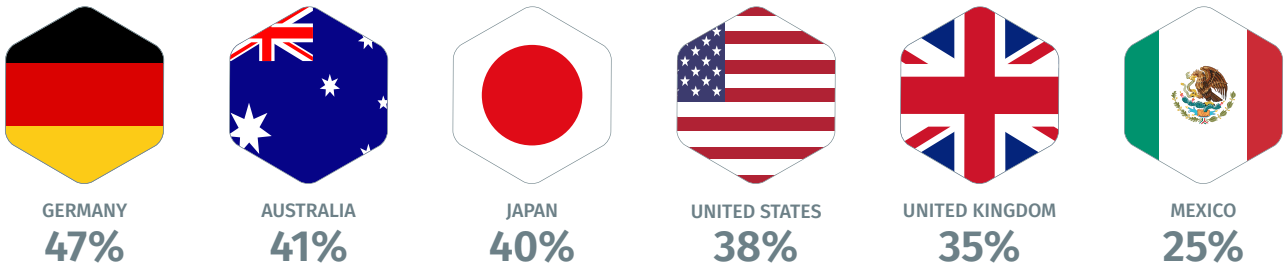
Figure 21. Does your organization measure the business costs of cyber risk?



Yes responses presented

German respondents are more likely to believe their measures of the business cost of cyber risk are accurate. Almost half (47 percent) of respondents in Germany rate the accuracy of their ability to measure the business costs of cyber risk as very accurate (7+ on a scale of 1 = not accurate to 10 = very accurate). Respondents in Mexico are far less likely to believe their measures are accurate. Only 25 percent of these respondents have confidence in their accuracy, as shown in Figure 22.

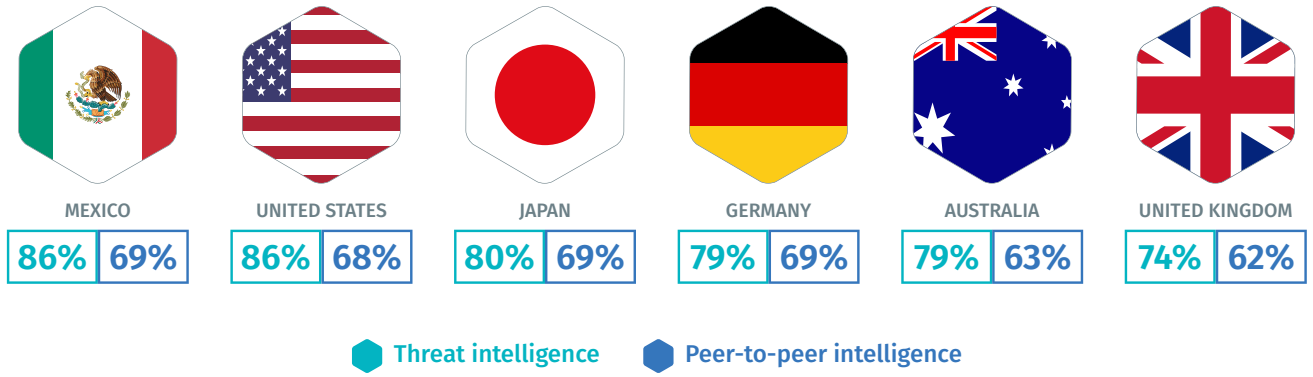
Figure 22. How accurate is your organization in measuring the business costs of cyber risks?



From 1 = not accurate at all to 10 = very accurate, 7+ responses presented

As shown in Figure 23, the countries most likely to believe threat intelligence is essential to prioritizing cyber risks are the US and Mexico (86 percent of respondents in both countries). The countries most likely to believe peer-to-peer intelligence is essential are Germany, Mexico and Japan (69 percent of respondents in all three countries).

Figure 23. How important is threat intelligence and peer-to-peer intelligence sharing?

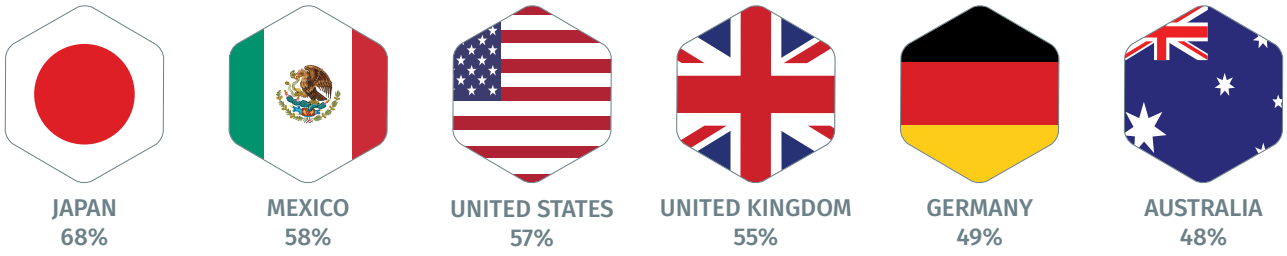


From 1 = not accurate at all to 10 = very accurate, 7+ responses presented

Certain countries are more likely to use non-security KPIs to measure the impact to business operations following a cyber attack.

According to Figure 24, 68 percent of Japanese respondents say their organizations use loss of revenue to measure the potential impact to business operations.

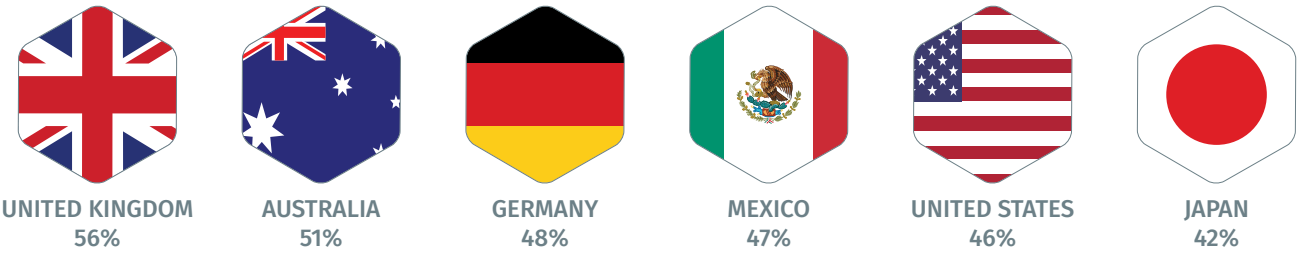
Figure 24. Is the loss of revenue a KPI for measuring the impact to business operations following a cyber attack?



Yes responses

Fifty-six percent of UK respondents say they use the loss of productivity to measure the impact to business operations following a cyber attack. Organizations in Japan are least likely to use this KPI (42 percent of respondents).

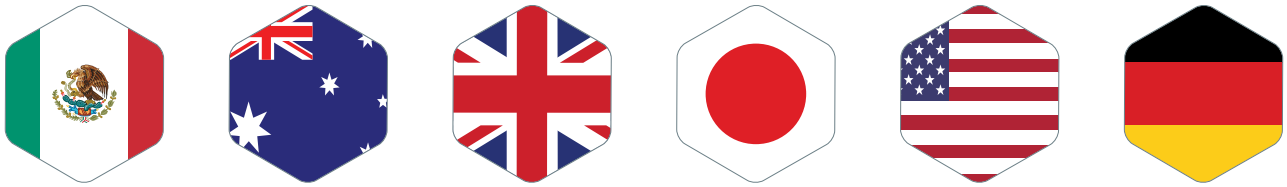
Figure 25. Is the loss of productivity a KPI for measuring the impact to business operations following a cyber attack?



Yes responses

Many companies are dependent upon manual processes to respond to vulnerabilities. According to Figure 26, 55 percent of respondents in Mexico agree their organizations are at a disadvantage in responding to vulnerabilities because of their dependency on manual processes. Fifty-three percent of respondents in Australia say reliance on manual processes is affecting their ability to respond to vulnerabilities.

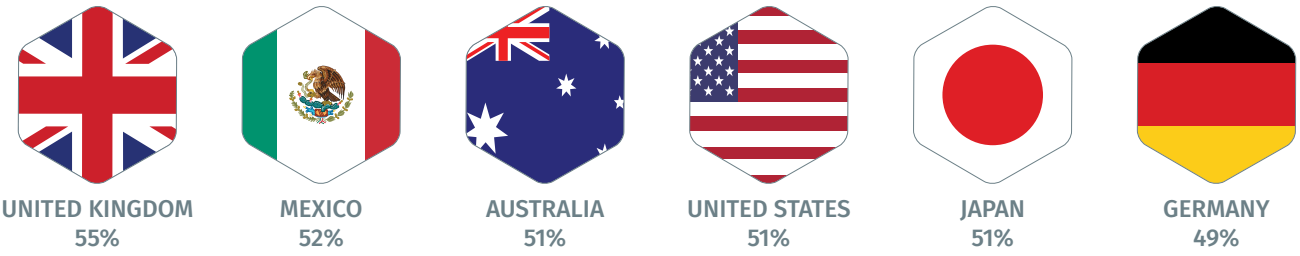
Figure 26. Our organization is at a disadvantage in responding to vulnerabilities because we use manual processes



Strongly agree and agree responses combined

Fifty-five percent of respondents in the UK say the use of manual processes is leading to an insurmountable response backlog. Less than half of respondents in Germany (49 percent) say issues with manual processes create an insurmountable response backlog, as shown in Figure 27.

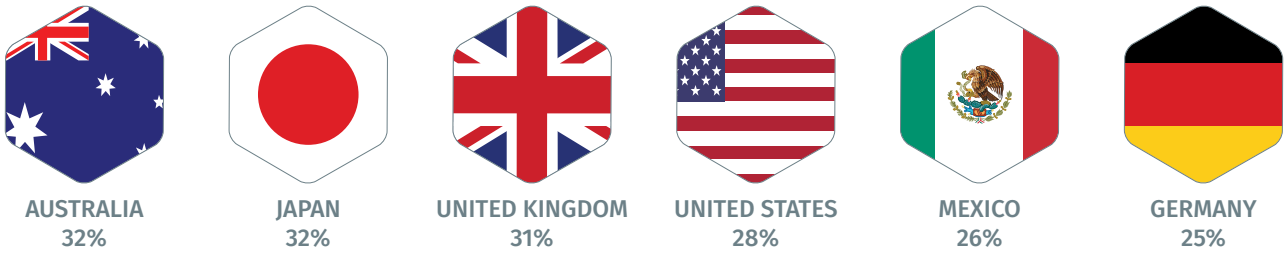
Figure 27. Security spends more time navigating manual processes than responding to vulnerabilities, which leads to an insurmountable response backlog.



Strongly agree and agree responses combined

Visibility into the attack surface is low in all countries. As shown in Figure 28, only 25 percent of respondents in Germany say they have sufficient visibility into their organization's attack surface.

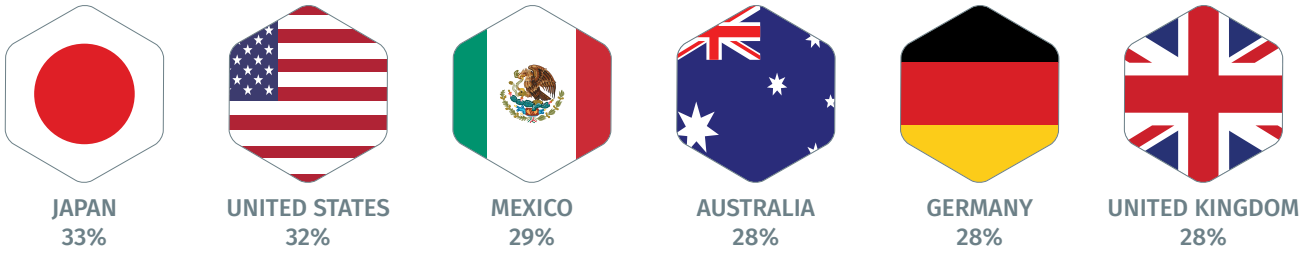
Figure 28. We have sufficient visibility into our organization's attack surface



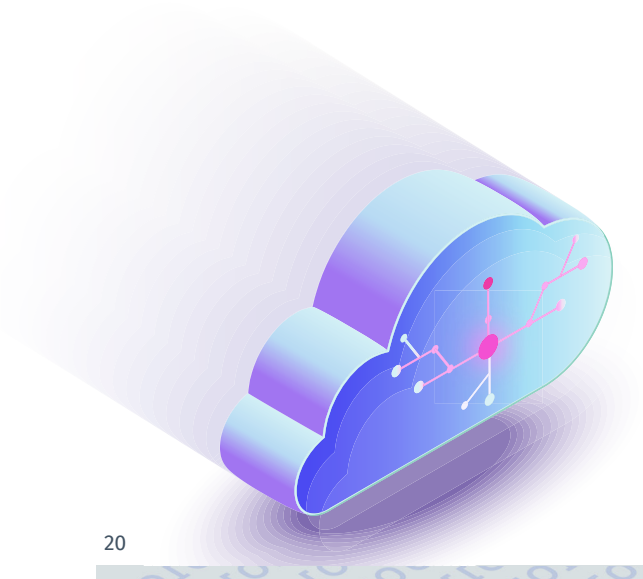
Strongly agree and agree responses combined

Most organizations in all countries are not able to correlate their cyber risk KPIs and the ability to mitigate the risk of a cyber attack. Only 28 percent of UK and German respondents say they are able to make these correlations to help them manage cyber risks, as presented in Figure 29.

Figure 29. We are able to correlate cyber risk KPIs and our ability to mitigate the risk of a data breach or security exploit.



Strongly agree and agree responses combined



Conclusion

According to the research, in 2019 respondents will be focused on improving their organizations' ability to keep up with the sophistication and stealth of attackers and protecting sensitive and confidential data from unauthorized access. To determine how best to achieve these goals, new approaches to measuring cyber risks are needed. Such measures should accurately quantify the consequences of cyber attacks.

Following are five recommendations, based on the research, for improving the ability to mitigate cyber risks.

1. Identify business operations and assets most vulnerable to cyber attacks, and be sure to include OT and IoT assets.

2. Utilize threat intelligence to prioritize remediation efforts in light of the overwhelming number of new vulnerabilities.

3. Identify the security gaps and opportunities to reduce complexity in the IT security infrastructure that leave organizations vulnerable to cyber attacks.

4. Measure the value of responding to vulnerabilities through automation and machine learning.

5. Better utilize IT security staff and resources to improve the efficiency of vulnerability management.

CISOs and security executives struggle to effectively communicate cyber risks to the CEO and boards of directors. The research also reveals a top governance priority for respondents is to have more frequent communications with their organizations' leadership. To achieve this goal, resources and time need to be allocated to the use of measures which will be helpful in making decisions in an understandable and actionable way.

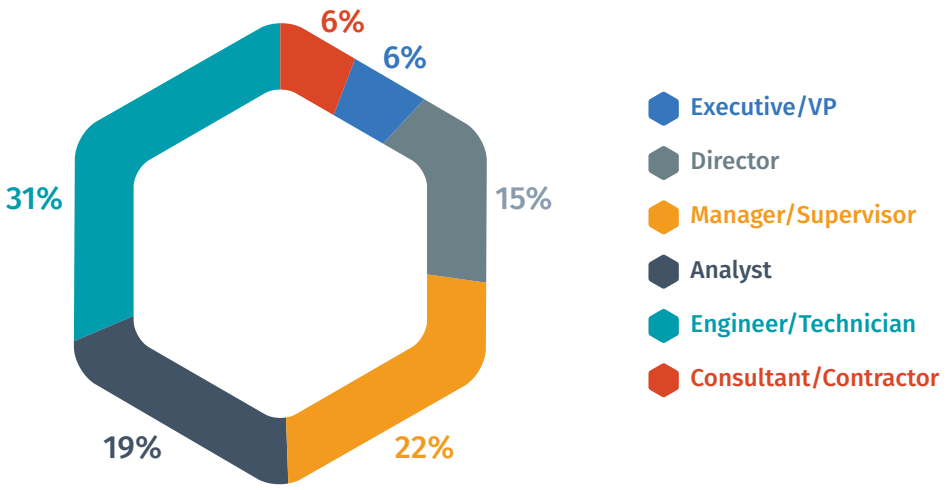
PART 3. METHODS

The sampling frame is composed of 64,871 IT and IT security practitioners in the United States, United Kingdom, Germany, Australia, Mexico and Japan. All respondents have a role in the evaluation and/or management of investments in cybersecurity solutions within their organization. As shown in Table 1, 2,691 respondents completed the survey. Screening removed 291 surveys. The final sample was 2,410 surveys (or a 3.7 percent response rate).

Table 1 Survey Response	Sampling Frame	Final Sample	Response Rate
United States	16,281	593	3.6%
United Kingdom	10,880	403	3.7%
Germany	11,006	427	3.9%
Australia	5,298	202	3.8%
Mexico	9,943	367	3.7%
Japan	11,463	418	3.6%
Total	64,871	2,410	3.7%

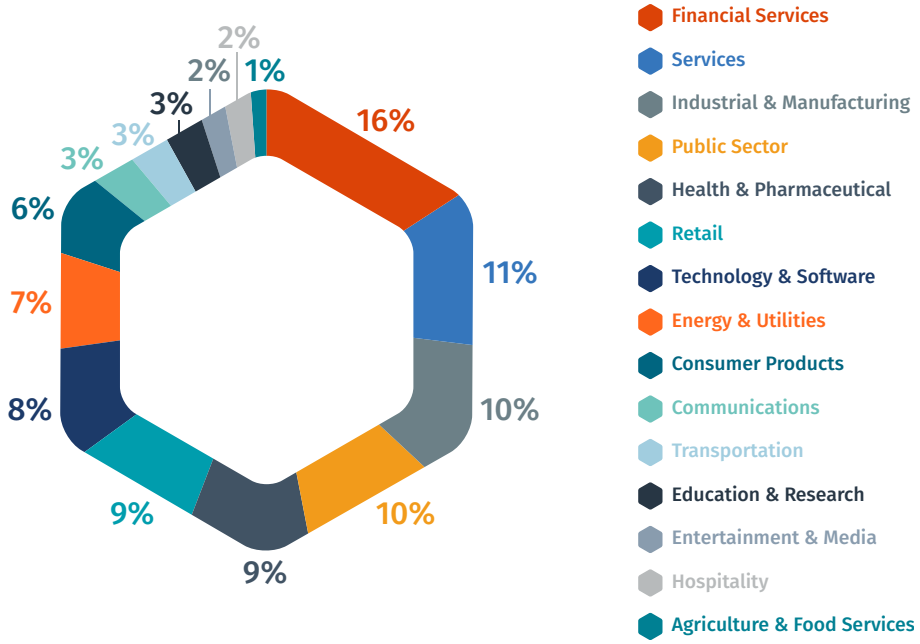
Pie Chart 1 reports the current position or organizational level of the respondents. Almost half of respondents (43 percent) reported their current position as supervisory or above and 31 percent of respondents are at the engineer/technician level.

Pie Chart 1. Distribution of respondents according to position level



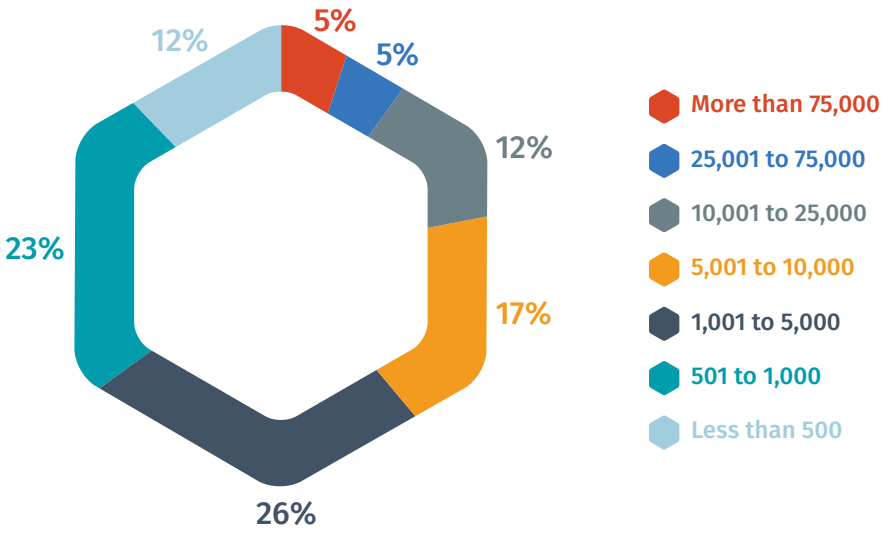
Pie Chart 2 reports the primary industry classification of respondents' organizations. This chart identifies financial services (16 percent of respondents) as the largest segment, followed by service sector (11 percent of respondents), industrial and manufacturing (10 percent of respondents), public sector (10 percent of respondents), health and pharmaceuticals (9 percent of respondents) and retail (9 percent of respondents).

Pie Chart 2. Distribution of respondents according to primary industry classification



According to Pie Chart 3, more than half of respondents (65 percent) are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 3. Distribution of respondents according to the number of employees within the organization



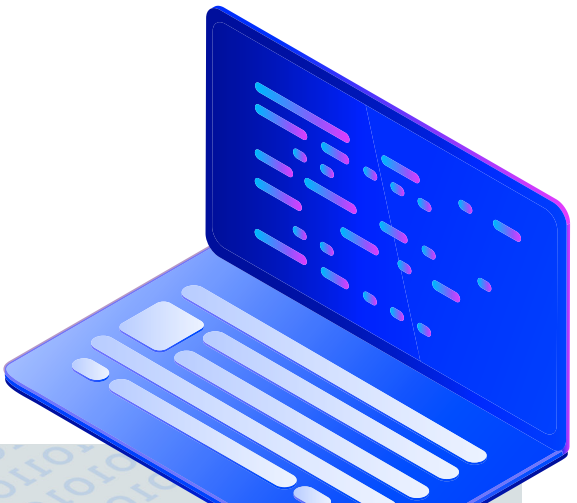
PART 4. CAVEATS

Inherent limitations to survey research need to be carefully considered before drawing inferences from findings. The following items are specific limitations 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 in the United States, United Kingdom, Germany, Australia, Mexico and Japan. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a specified time period.

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.



Appendix: 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 November 1, 2018 and November 9, 2018.

Survey Response	Total
Total sampling frame	64,871
Total returns	2,691
Rejected surveys	291
Final sample	2,410
Response rate	3.7%

PART 1. BACKGROUND

S1. What best describes your involvement in the evaluation and/or management of investments in cybersecurity solutions within your organization	Total
None (stop)	0%
Responsible for evaluating investments	30%
Responsible for managing investments	37%
Some involvement in evaluating solutions	39%
Some involvement in managing investments	38%
Total	**144%**

S2. What best describes your role within your organization's IT or IT security department or function?	Total
Security leadership (CISO)	36%
IT management	31%
IT operations	42%
Security management	36%
Security architecture	10%
Incident response	50%
SOC administration	40%
Compliance	17%
Applications development (AppSec)	15%
I'm not involved in my organization's IT or IT security function (stop)	0%
Total	**277%**

S3. How knowledgeable are you about your organization's vulnerability management program?	Total
Very knowledgeable	30%
Knowledgeable	40%
Somewhat knowledgeable	29%
Slightly knowledgeable (stop)	0%
No knowledge (stop)	0%
Total	**100%**

PART 2. CYBERSECURITY RISKS

Q1a. Does your organization measure the business costs of cyber risk?	Total
Yes	46%
No	54%
Total	**100%**

Q1b. If yes, is security required to report the results to the board of directors?	Total
Yes	41%
No	59%
Total	**100%**

Q1c. If yes, how accurate is your organization in measuring the business costs of cyber risk using the 10-point scale from 1 = not accurate at all to 10 = very accurate.	Total
1 or 2	22%
3 or 4	22%
5 or 6	19%
7 or 8	23%
9 or 10	15%
Total	**100%**
Extrapolated value	*5.25*

Follwing are seven key performance indicators (KPIs) that may be related to cyber risk within your oganization.

Q2a. Is time to assess cyber risk a KPI used by your organization?	Total
Yes	49%
No	51%
Total	**100%**

Q2b. If yes, please rate the importance of this KPI for mitigating or minimizing cyber risk using the 10-point scale from 1 = not important at all to 10 = essential.	Total
1 or 2	8%
3 or 4	10%
5 or 6	18%
7 or 8	32%
9 or 10	32%
Total	**100%**
Extrapolated value	*6.90*

Q3a. Is time to remediate cyber risk a KPI used by your organization?	Total
Yes	46%
No	54%
Total	**100%**

Q3b. If yes, please rate the importance of this KPI for mitigating or minimizing cyber risk using the 10-point scale from 1 = not accurate at all to 10 = essential.	Total
1 or 2	7%
3 or 4	10%
5 or 6	13%
7 or 8	33%
9 or 10	37%
Total	**100%**
Extrapolated value	*7.13*

Q4a. Is identifying OT and IoT assets a KPI used by your organization?	Total
Yes	34%
No	65%
Total	**100%**

Q4b. If yes, please rate the importance of this KPI for mitigating or minimizing cyber risk using the 10-point scale from 1 = not important at all to 10 = essential.	Total
1 or 2	10%
3 or 4	11%
5 or 6	16%
7 or 8	26%
9 or 10	36%
Total	**100%**
Extrapolated value	*6.84*

Q5a. Is prioritization effectiveness a KPI used by your organization?	Total
Yes	30%
No	70%
Total	**100%**

Q5b. If yes, please rate the importance of this KPI for mitigating or minimizing cyber risk using the 10-point scale from 1 = not important at all to 10 = essential.	Total
1 or 2	13%
3 or 4	11%
5 or 6	18%
7 or 8	29%
9 or 10	28%
Total	**100%**
Extrapolated value	*6.45*

Q6a. Is the drop in your organization's stock price a KPI for measuring the impact to business operations following a cyber attack?	Total
Yes	12%
No	88%
Total	**100%**

Q6b. If yes, please rate the importance of this KPI using the 10-point scale from 1 = not important at all to 10 = essential.	Total
1 or 2	20%
3 or 4	18%
5 or 6	21%
7 or 8	23%
9 or 10	17%
Total	**100%**
Extrapolated value	*5.48*

Q7a. Is the loss of revenue a KPI for measuring the impact to business operations following a cyber attack?	Total
Yes	56%
No	43%
Total	**100%**

Q7b. If yes, please rate the importance of this KPI using the 10-point scale from 1 = not important at all to 10 = essential.	Total
1 or 2	6%
3 or 4	9%
5 or 6	17%
7 or 8	33%
9 or 10	35%
Total	**100%**
Extrapolated value	*7.13*

Q8a. Is the loss of productivity a KPI for measuring the impact to business operations following a cyber attack?	Total
Yes	48%
No	52%
Total	**100%**

Q8b. If yes, please rate the importance of this KPI using the 10-point scale from 1 = not important at all to 10 = essential.	Total
1 or 2	8%
3 or 4	10%
5 or 6	13%
7 or 8	39%
9 or 10	31%
Total	**100%**
Extrapolated value	*7.02*

Q9. Has your organization experienced any of the following in the past 24 months? Please select all that apply.	Total
A cyber attack that caused significant downtime	35%
A nation state attack	15%
A data breach involving 10,000 or more customer or employee records	31%
Leakage of business confidential information, such as emails	34%
An attack that involved IoT or OT assets	23%
An attack against OT infrastructure that resulted in downtime to plant and/or operational equipment	28%
Cyber extortion such as ransomware	30%
Economic espionage (theft of business-critical information)	29%
Fines and/or lawsuits for non-compliance with data protection and privacy requirements	18%
A third party misued or shared confidential information with other third parties	41%
A significant disruption to business processes caused by malware	48%
A careless employee fell for a phishing scam that resulted in credential theft	67%
Other	5%
Total	**404%**

Q10. Which of the following threats do you worry about in 2019? Please select the top five threats.	Total
A cyber attack that causes significant downtime	39%
A nation state attack	13%
A data breach involving 10,000 or more customer or employee records	52%
Leakage of business confidential information, such as emails	47%
An attack that involved IoT or OT assets	56%
An attack against my company's OT infrastructure that results in downtime to plant and/or operational equipment	48%
Cyber extortion such as ransomware	27%
Economic espionage (theft of business-critical information)	44%
Fines and/or lawsuits for non-compliance with data protection and privacy requirements	16%
A third party misuses or shares confidential information with other third parties	64%
A significant disruption to business processes caused by malware	54%
A careless employee falls for a phishing scam that resulted in credential theft	40%
Other	1%
Total	**500%**

Q11a. Does your organization attempt to quantify the damage these events could have on its business?	Total
Yes	41%
No	59%
Total	**100%**

Q11b. If yes, what factors are used to quantify the risk? Please select all that apply.	Total
Financial loss	43%
Decline in stock price	15%
Employee turnover	24%
Customer turnover	35%
Loss of market share	28%
Theft of intellectual property	54%
Frequency of unpatched (known) vulnerabilities	41%
Downtime of OT systems	31%
Loss of employee productivity	42%
Other	2%
Total	**316%**

Q12. What are your governance priorities for 2019? Please select all that apply.	Total
Allocate more resources to vulnerability management	47%
Increase the number of FTEs in our IT security function	48%
Ensure third parties have appropriate security practices to protect sensitive and confidential data	67%
Increase communication with C-level and board of directors about the cyber threats facing our organization	64%
Increase staff training to prevent careless behavior such as falling for a phishing scam or sharing passwords	53%
Other	1%
Total	**281%**

Q13. What are your security priorities for 2019? Please select all that apply.	Total
Control the proliferation of IoT devices in the workplace	25%
Reduce the risk of unsecured IoT devices in the workplace	37%
Reduce the risk of attacks to the OT infrastructure	40%
Improve controls over third parties' access to our sensitive and confidential data	42%
Improve protection of sensitive and confidential data from unauthorized access	48%
Improve our ability to keep up with the sophistication and stealth of the attackers	61%
Reduce complexity in our IT security infrastructure	60%
Other	3%
Total	**364%**

Q14. Please rank your priorities for measuring and managing the cyber risk for 2019 in the following asset types from 1 = highest priority to 6 = lowest priority. Please avoid a tied score.	Total
IT infrastructure (e.g. servers, desktops, laptops, mobile and virtual machines)	2.45
Web applications	1.90
Cloud infrastructure	1.70
Containers	4.90
IoT	2.80
Operational technology (e.g. PLCs, RTUs and HMI)	4.55

Q15. How important is threat intelligence to setting cybersecurity priorities within your organization? Please use the following 10-point scale from 1 = not important at all to 10 = essential.	Total
1 or 2	5%
3 or 4	5%
5 or 6	9%
7 or 8	31%
9 or 10	49%
Total	**100%**
Extrapolated value	*7.82*

Q16. How important is peer-to-peer intelligence sharing and collaboration to setting cybersecurity priorities within your organization? Please use the following 10-point scale from 1 = not important at all to 10 = essential.	Total
1 or 2	11%
3 or 4	10%
5 or 6	12%
7 or 8	24%
9 or 10	43%
Total	**100%**
Extrapolated value	*7.06*

Q17a. Does your organization's senior management involve security when evaluating new platforms/systems?	Total
Yes	37%
No	63%
Total	**100%**

Q17b. If yes, who is most involved in the evaluation of cyber risk as part of your organization's business risk management?	Total
Chief Information Officer	36%
Chief Information Security Officer	17%
Chief Security Officer	4%
Chief Risk Officer	7%
Chief Technology Officer	9%
Line of Business (LoB) Management	20%
Plant management	5%
Other	1%
Total	**100%**

Attributions: Please use the scale from strongly agree to strongly disagree below each item. Strongly Agree and Agree responses combined.	Total
Q18a. The security function in our organization has adequate staffing to scan vulnerabilities in a timely manner.	42%
Q18b. Investments in security technologies are based on what our peers are spending and the technologies they are purchasing.	35%
Q18c. Investments in security technologies are influenced by media coverage of data breaches and cyber exploits.	41%
Q18d. Our organization is at a disadvantage in responding to vulnerabilities because we use manual processes.	48%
Q18e. Security spends more time navigating manual processes than responding to vulnerabilities, which leads to an insurmountable response backlog.	51%
Q18f. We incorporate threat intelligence into prioritizing assets that are most important to safeguard.	39%
Q18g. We have sufficient visibility into our organization's attack surface (i.e. cloud, containers, IoT and OT).	29%
Q18h. We are able to correlate cyber risk KPIs and our ability to mitigate the risk of a data breach or security exploit.	30%
Q18i. Traditional KPIs or metrics for evaluating business risk do not work for evaluating cyber risks.	58%

Q19. What role does your CISO play in vulnerability management within your organization?	Total
Determine strategy for managing vulnerabilities	38%
Determine investments in vulnerability management technologies	44%
Lead patch management process	51%
None	27%
Other	3%
Total	**163%**

Q20. How many employees (FTEs) are involved in vulnerability management within your organization?	Total
Less than 5	12%
5 to 10	21%
11 to 20	28%
21 to 30	21%
31 to 40	11%
41 to 50	5%
More than 50	2%
Total	**100%**
Extrapolated value	*18.8*

Q21. Does your organization conduct ad hoc vulnerability scans in response to the public disclosure of a major new vulnerability?	Total
Yes	48%
No	49%
Don't know	4%
Total	**100%**

Q22. How quickly does your organization scan for vulnerabilities once they have been publicly disclosed?	Total
More than once per day	7%
Daily	8%
Between 2 and 3 times per week	6%
Every week	5%
Every 2 weeks	6%
Every 3 weeks	3%
Every 4 weeks	1%
More than 4 weeks	4%
No set schedule	31%
We don't scan	28%
Total	**100%**

Q23. What determines the frequency of scanning? Please select all that apply.	Total
Availability of resources	32%
Availability of threat intelligence	44%
Assessment of risks to sensitive data	35%
Prioritization of cyber risks	46%
Comparison to peers in other companies	25%
Concerns about business disruption	20%
Other	1%
Total	**203%**

Q24. How does your organization scan for vulnerabilities currently?	Total
Mostly a manual process	31%
Mostly an automated process	34%
Combination of manual and automated process	35%
Total	**100%**

Q25. Does your organization plan to utilize artificial intelligence (AI) and machine learning (ML)?	Total
Currently deploying AI and ML solutions	14%
Planning to deploy AI and ML solutions with the next 12 months	29%
Planning to deploy AI and ML solutions within 12 to 24 months	19%
No plan to deploy AI and ML	39%
Total	**100%**

Q26a. How effective is your organization's vulnerability management program at mitigating or minimizing the success of a cyber attack?	Total
1 or 2	8%
3 or 4	13%
5 or 6	19%
7 or 8	27%
9 or 10	33%
Total	**100%**
Extrapolated value	*6.79*

Q26b. If very effective, why? Please check all that apply.	Total
We have the ability to quickly assess vulnerabilities and other threats	45%
We have the ability to quickly remediate security exploits and/or data breaches	51%
We have the ability to assess vulnerabilities in all critical IT, OT and IoT assets	51%
Other	4%
Total	**151%**

Q27a. How effective is your organization's ability to prioritize threats to critical business assets?	Total
1 or 2	13%
3 or 4	12%
5 or 6	16%
7 or 8	31%
9 or 10	28%
Total	**100%**
Extrapolated value	*6.43*

Q27b. If very effective, why? Please check all that apply.	Total
We have the ability to quickly assess vulnerabilities	47%
We have the ability to quickly remediate security exploits and/or data breaches	55%
We have the ability to assess vulnerabilities in all critical IT, OT and IoT assets	46%
Other	5%
Total	**152%**

Q28. How does your organization prioritize threats to critical business assets? Please select all that apply.	Total
CVSS	39%
Ease of remediation	41%
Criticality of impacted systems	44%
None of the above	27%
Other	5%
Total	**157%**

Q29a. Does your organization benchmark its ability to prioritize cyber threats (with comparison to other companies in the same industry, size and/or geographic footprint)?	Total
Yes	38%
No	62%
Total	**100%**

Q29b. If no, does your organization plan to benchmark its capability to prioritize threats in the future?	Total
Yes	33%
No	67%
Total	**100%**

PART 3. DEMOGRAPHICS

D1. What best describes your position within the organization?	Total
Executive/VP	6%
Director	15%
Manager/Supervisor	22%
Analyst	19%
Engineer/Technician	31%
Consultant/Contractor	6%
Other	0%
Total	**100%**

D2. What best describes your organization's primary industry classification?	Total
Agriculture & food services	1%
Communications	3%
Consumer products	6%
Defense & aerospace	0%
Education & research	2%
Energy & utilities	7%
Entertainment & media	2%
Financial services	16%
Health & pharmaceutical	9%
Hospitality	2%
Industrial & manufacturing	10%
Public sector	10%
Retail	9%
Services	11%
Technology & software	8%
Transportation	3%
Other	0%
Total	**100%**

D3. What range best describes the full-time headcount of your global organization?	Total
Less than 500	12%
501 to 1,000	23%
1,001 to 5,000	26%
5,001 to 10,000	17%
10,001 to 25,000	12%
25,001 to 75,000	5%
More than 75,000	5%
Total	**100%**

Please write to **research@ponemon.org** or call **800.887.3118** if you have any questions.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advance 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.

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.

7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046

North America +1 (410) 872-0555

www.tenable.com