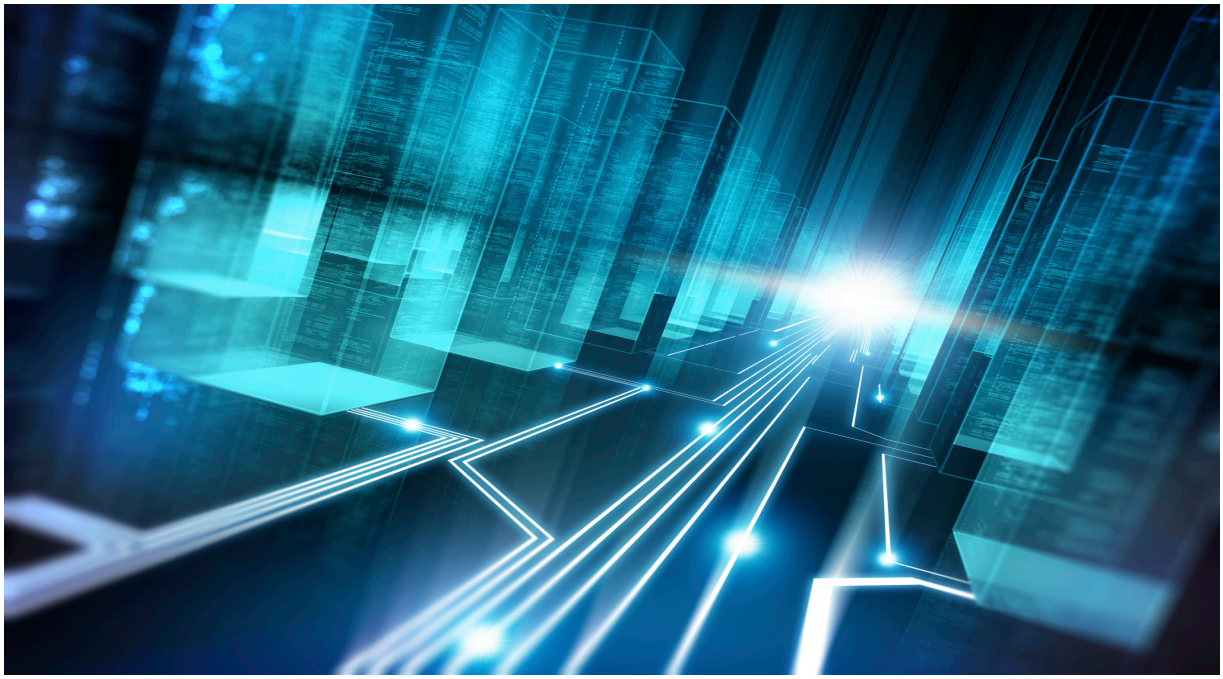


Reducing Cybersecurity Costs & Risk through Automation Technologies

Sponsored by Juniper Networks

Independently conducted by Ponemon Institute LLC

Publication Date: November 2017

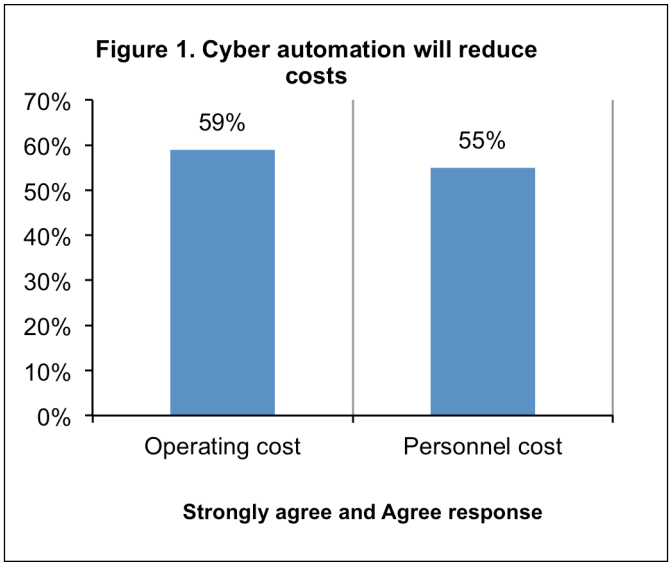
Reducing Cybersecurity Costs & Risk through Automation Technologies

Ponemon Institute: November 2017

Part 1. Introduction

Cyber automation refers to enabling security technologies that augment or replace human intervention in the identification and containment of cyber exploits or breaches. Such technologies depend upon artificial intelligence, machine learning and orchestration. The purpose of this study, *Reducing Cybersecurity Costs & Risk through Automation Technologies,* is to understand how organizations are deploying these technologies, the benefits of automation and their cost-effectiveness.

A key takeaway from this research (as shown in Table 1 of this report) is evidence that cyber automation reduces the required hours to deal with security exploits with greater accuracy and as a result can save organizations an average of more than $2.3 million annually while strengthening their security posture.



As shown in Figure 1, the majority of respondents believe cyber automation reduces both operating and personnel costs (59 percent and 55 percent of respondents, respectively).

In this study, we surveyed 1,524 IT and IT security practitioners in the United States, EMEA and Asia-Pac. All respondents are familiar with their organizations' practices for identifying and/or containing cyber events and have some level of responsibility in directing security program activities and making investments in "next generation" security technologies.

Following are key findings from this study.

Migration to the cloud has increased the need for automation of cyber tools and technologies. As more companies move their IT infrastructure to the cloud, enhanced security, such as cyber automation, is increasing in importance, according to 59 percent of respondents.

Companies are committed to the deployment of cyber automation. Most companies represented in this research (61 percent of respondents) are committed to at some point having cyber automation as part of their security arsenals. One reason, according to 62 percent of respondents, is that the use of cyber automation will reduce the rate of false positives in the investigation of security alerts.

Complexity is a barrier to full deployment. On the downside, 60 percent of respondents say the integration of cybersecurity automation within their companies' existing IT security architectures is a complex and time-consuming process.

Automated tools and technologies reduce the need for human intervention in the containment of cyber exploits. In this research, 53 percent of respondents say their organizations have automated tools and/or technologies that capture intelligence and evaluate

the true threat posed by cyber attackers. According to respondents, an average of 51 percent of cyber exploits or the containment of malware can be handled without human intervention.

Companies are slow to rely on automated tools such as machine learning and artificial intelligence. More than half of companies represented have automated tools. However, only 20 percent of respondents say their organizations' approach to cyber defense primarily relies on these technologies. Instead, 34 percent say they rely primarily on manual activities and 25 percent of respondents say their approach is "ad hoc" or not specified.

Will automation replace IT security staff? Most senior managers, according to 60 percent of respondents, do not believe smart machines will replace skilled security personnel and 71 percent of respondents say cyber automation will never fully replace human involvement and expertise. An average of almost 17 security staff members are involved in the cyber exploit or malware containment process and they have an average of 8.5 years of experience.

Cyber automation technologies will help organizations address their staffing concerns. Fifty-five percent of respondents say the use of cyber automation will reduce personnel costs and 53 percent of respondents say the inability to properly staff skilled security personnel has increased investments in the automation of cyber tools and technologies. In addition to reducing personnel costs, operating costs will be reduced as well (59 percent of respondents).

Part 2. Key findings

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

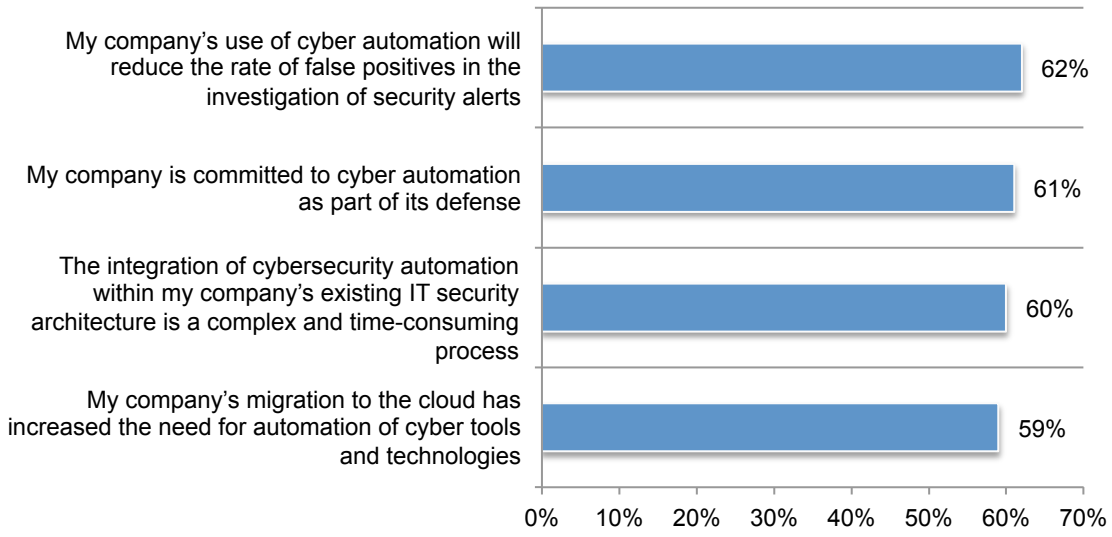
- Perceptions about the value of cyber automation
- Cyber defense and cyber automation
- Impact of automation on staffing and cost

Perceptions about the value of cyber automation

Migration to the cloud has increased the need for automation of cyber tools and technologies. According to Figure 2, as more companies move their IT infrastructure to the cloud, enhanced security, such as cyber automation, is increasing in importance, according to 59 percent of respondents.

Most companies represented in this research (61 percent of respondents) are committed to at some point having cyber automation as part of their security arsenals. An important benefit, according to 62 percent of respondents, is that the use of cyber automation will reduce the rate of false positives in the investigation of security alerts. On the downside, 60 percent of respondents say the integration of cybersecurity automation within their companies' existing IT security architectures is a complex and time-consuming process.

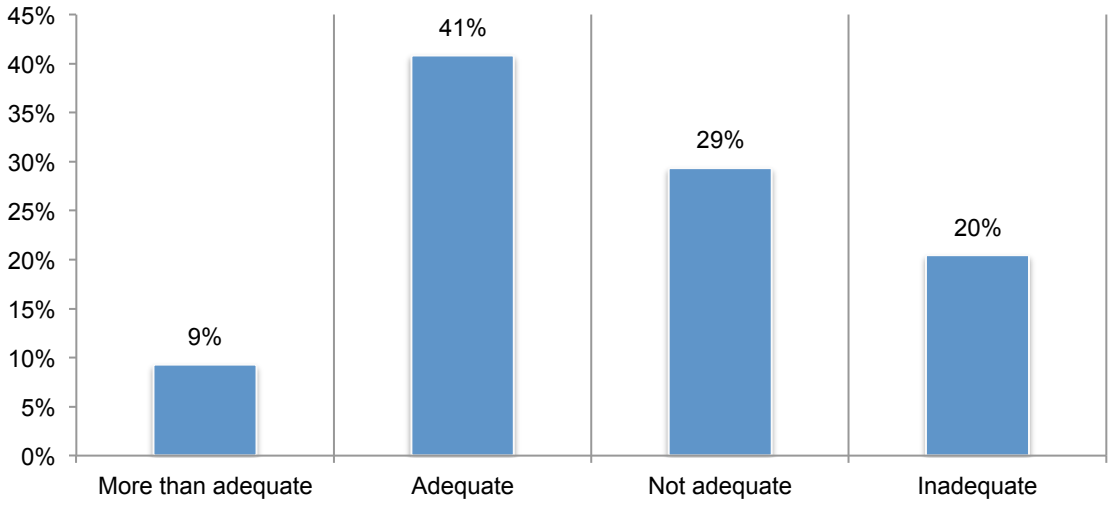
Figure 2. Perceptions about the value of cyber automation
Strongly agree and Agree responses combined



Automated tools and technologies reduce the need for human intervention in the containment of cyber exploits. In this research, 53 percent of respondents say their organizations have automated tools and/or technologies that capture intelligence and evaluate the true threat posed by cyber attackers. According to respondents, an average of 51 percent of cyber exploits or the containment of malware can be handled without human intervention.

As shown in Figure 3, of the 53 percent of respondents that say their organization has automated tools, 50 percent of those respondents say the automated tools and/or technologies are more than adequate (9 percent) or adequate (41 percent).

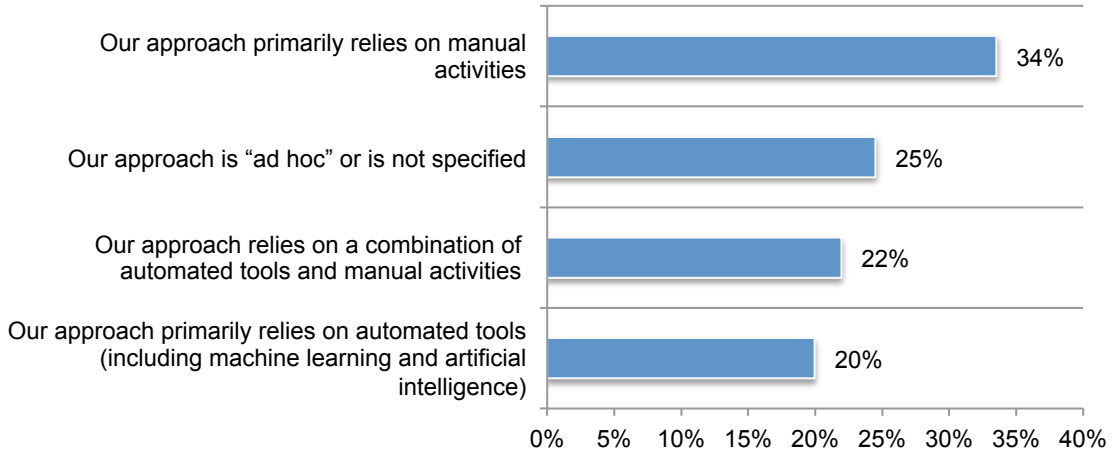
Figure 3. What best describes the adequacy of automated tools and/or technologies deployed by your organization?



Cyber defense and cyber automation

Companies are slow to rely on automated tools such as machine learning and artificial intelligence. More than half of companies represented have automated tools. However, as shown in Figure 4, only 20 percent of respondents say their organizations' approach to cyber defense primarily relies on these technologies. Instead, 34 percent say they rely primarily on manual activities and 25 percent of respondents say their approach is "ad hoc" or not specified.

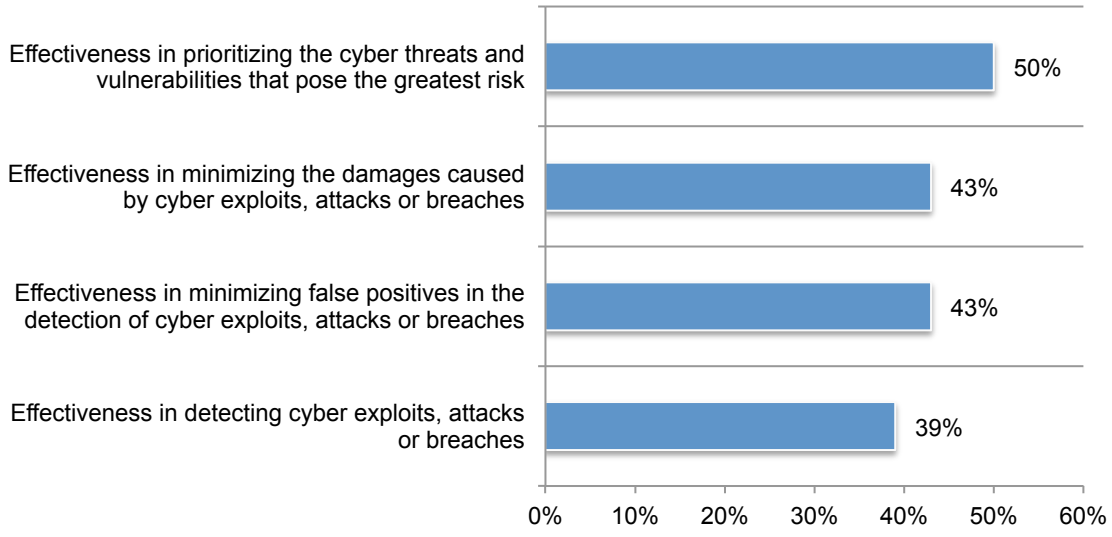
Figure 4. What best describes your organization's approach to cyber defense?



The continued use of manual activities may keep many organizations from being more effective in detecting cyber attacks and minimizing their consequences. As shown in Figure 5, when asked to rate the effectiveness of their organizations' cyber defense on a scale of 1 = low effectiveness to 10 = high effectiveness, 43 percent of respondents rate their effectiveness in minimizing false positives in the detection of cyber exploits, attacks or breaches and minimizing the damages caused by cyber exploits, attacks or breaches as highly effective (7+ on a scale of 1 = low effectiveness to 10 = high effectiveness).

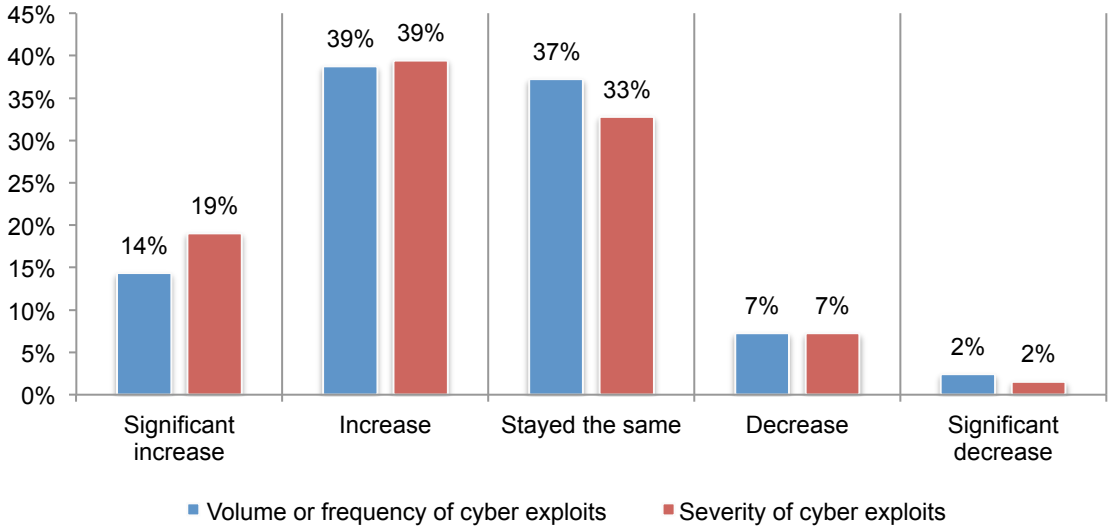
However, only 39 percent of respondents say they are highly effective in detecting cyber exploits, attacks or breaches. More respondents (50 percent) rate their organizations' effectiveness in prioritizing the cyber threats and vulnerabilities that pose the greatest risk as highly effective.

Figure 5. Effectiveness in detecting cyber exploits, minimizing false positives and the damages caused by cyber exploits and prioritizing cyber threats
1 = low effectiveness to 10 = high effectiveness, 7+ responses reported



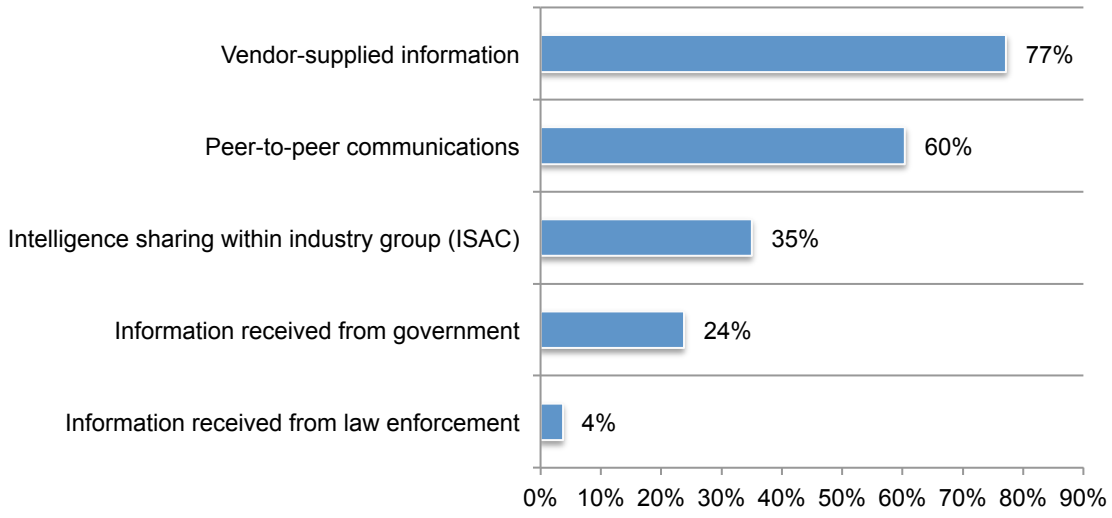
Low effectiveness in dealing with cyber exploits indicates companies may not be able to keep pace with increases in the volume and severity of cyber crime. More than half (53 percent of respondents) say cyber exploits have increased over the past 12 months and 58 percent of respondents say the severity of these incidents have increased, according to Figure 6.

Figure 6. How has the volume or frequency of cyber exploits changed in the past 12 months?



As shown in Figure 7, the main intelligence sources used in cyber defense are vendor-supplied information and peer-to-peer communications (77 percent and 60 percent of respondents, respectively). In a typical week, an average of 518 cybersecurity alerts are actually investigated and an average of 34 percent of cyber exploits or malware infections go undetected because they bypass the organizations' IPS and/or AV systems.

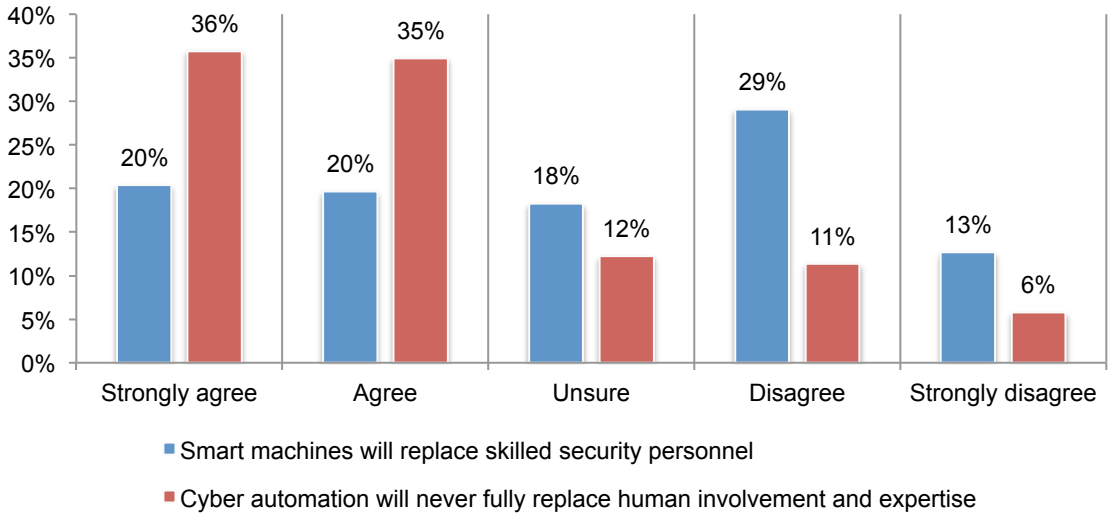
Figure 7. The main intelligence sources used by organizations' cyber defense
Two responses permitted



Impact of automation on staffing and cost

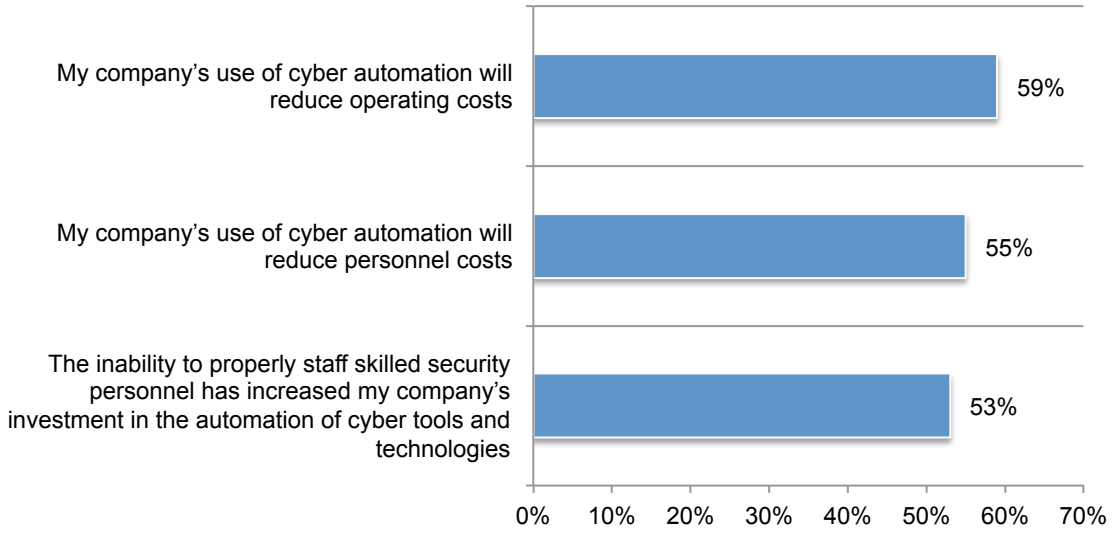
Will automation replace IT security staff? Most senior managers, according to 60 percent of respondents, do not believe smart machines will replace skilled security personnel and 71 percent of respondents say cyber automation will never fully replace human involvement and expertise, according to Figure 8. An average of almost 17 security staff members are involved in the cyber exploit or malware containment process and they have an average of 8.5 years of experience.

Figure 8. The impact of cyber automation on staffing



Cyber automation technologies will help organizations address their staffing concerns. As presented in Figure 9, 55 percent of respondents say the use of cyber automation will reduce personnel costs and 53 percent of respondents say the inability to properly staff skilled security personnel has increased investments in the automation of cyber tools and technologies. In addition to reducing personnel costs, operating costs will be reduced as well (59 percent of respondents).

Figure 9. The benefits of cyber automation
Strongly agree and Agree responses combined



The use of automation is shown to reduce the time to deal with cyber exploits. As shown in Table 1, when automation is used to contain cyber exploits, the time and cost are significantly reduced. The average cost of not using cyber automation to address cyber exploits is almost $3 million versus $646,425 if cyber automation is used. Thus, a company can potentially save an average of more than $2.3 million in operating costs.

According to the research, malware alerts are rarely reliable. An average of 12,172 malware alerts are received in the typical week. Twenty-one percent of these alerts are reliable and 20 percent of these alerts pertain to advanced persistent threats. However, as shown in the table, cyber automation can significantly reduce the costs of capturing, evaluating and investigating intelligence about cyber exploits or malware.

Table 1. Labor hours spent containing cyber exploits	Not facilitated by automation	Facilitated by automation	Difference in hours
Organizing and planning approaches to cyber defense	16.6	9.7	6.9
Capturing actionable intelligence about cyber exploits and malware infections	73.2	36.4	36.8
Evaluating actionable intelligence about cyber exploits or malware	49.7	14.7	35.0
Investigating actionable intelligence about cyber exploits or malware	177.4	55.1	122.3
Cleaning, fixing and/or patching networks, applications and devices (i.e., endpoints) damaged/infected by cyber exploits or malware	195.2	36.9	158.3
Documenting and/or reporting upon the cyber event (in conformance with policies or compliance mandates)	14.0	6.9	7.1
Time wasted by security staff members chasing erroneous or false positives	390.4	38.1	352.3
Total hours per week	916.5	197.8	718.7
Total hours per year	47,658	10,286	37,372
Estimated total cost per year	$2,978,625*	$642,850*	$2.335.775*

*IT and IT security fully loaded pay rate is $62.50 (source: Ponemon Institute).

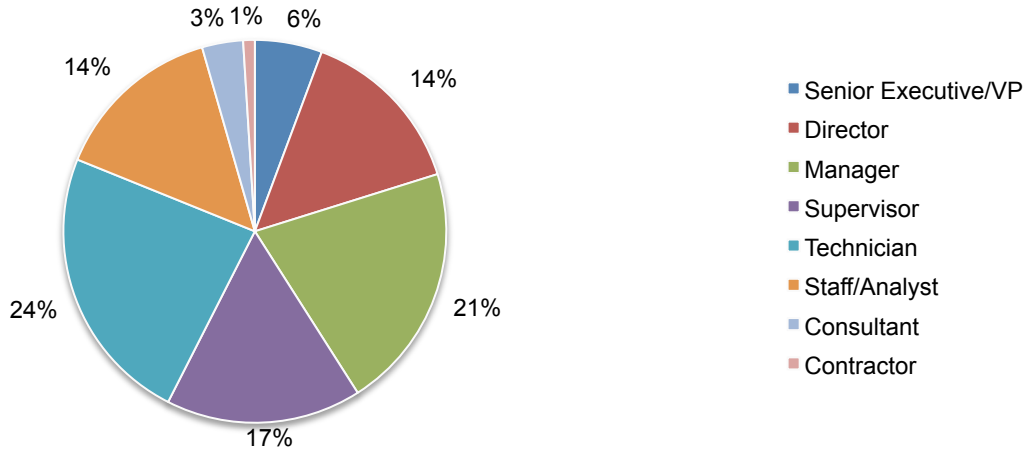
Part 3. Methods

A sampling frame of 43,970 experienced IT and IT security practitioners located in the United States, EMEA and Asia-Pac, who are familiar with their organizations' practices for identifying and/or containing cyber events and have some level of responsibility in directing security activities and investments, were selected as participants in the research. Table 2 shows 1,679 total returns. Screening and reliability checks required the removal of 155 surveys. Our final sample consisted of 1,524 surveys or a 3.5 percent response.

Table 1. Sample response	Consolidated
Sampling frame	43,970
Total returns	1,679
Rejected or screened surveys	155
Final sample	1,524
Response rate	3.5%

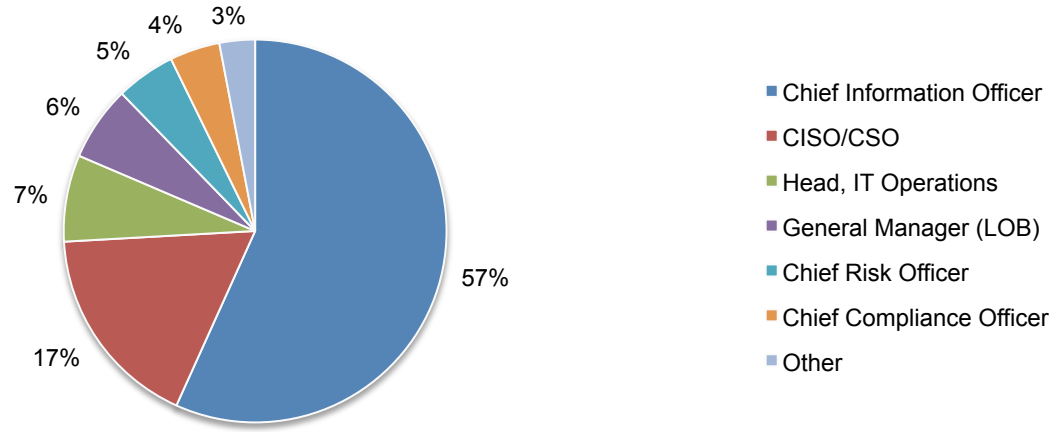
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, 58 percent of respondents are at or above the supervisory levels.

Pie Chart 1. Current position within the organization



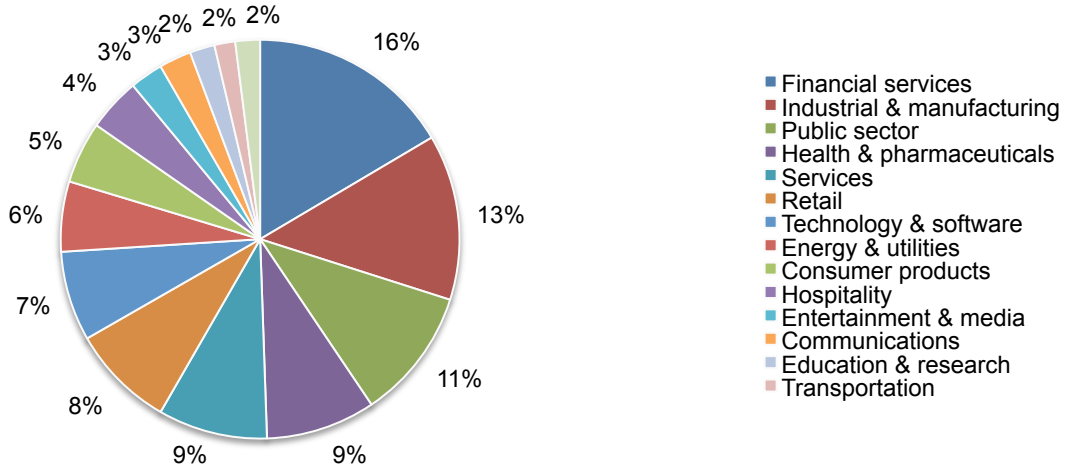
As shown in Pie Chart 2, 57 percent of respondents report to the CIO and 17 percent of respondents report to the CISO/CSO.

Pie Chart 2. Primary person reported to within the organization



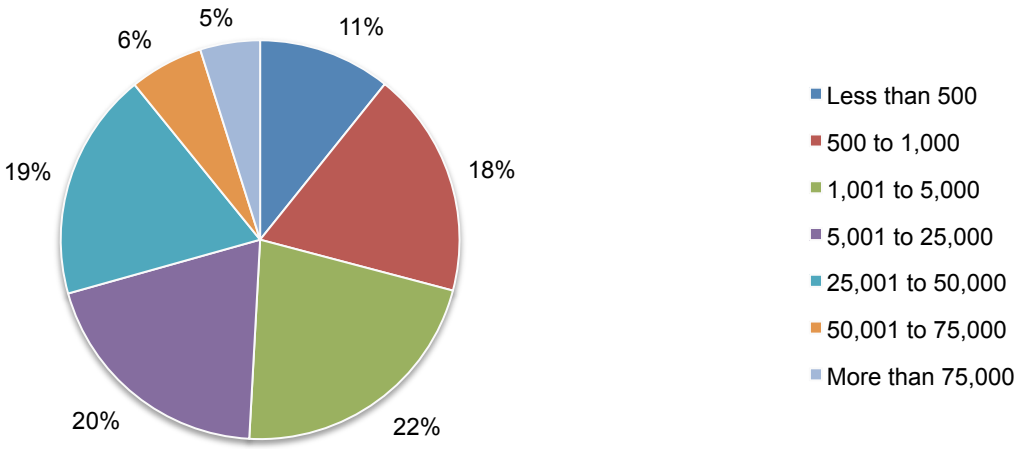
Pie Chart 3 reports the industry classification of respondents' organizations. This chart identifies financial services (16 percent) as the largest segment, followed by industrial and manufacturing organizations (13 percent) and the public sector (11 percent).

Pie Chart 3. Primary industry focus



As shown in Pie Chart 4, 72 percent of respondents are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 4. Global employee headcount



Part 4. 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.

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 August 14 and September 12, 2017.

Survey response	Consolidated data
Total sampling frame	43,970
Total returns	1,679
Rejected surveys	155
Final sample	1,524
Response rate	3.5%
Sample weights	1.00

Part 1. Screening questions

S1. How familiar are you with your organization's practices for identifying and/or containing cyber events?	Consolidated data
Very familiar	38%
Familiar	36%
Somewhat familiar	26%
No knowledge (Stop)	0%
Total	100%

S2. Do you have any responsibility for directing security activities and investments in your organization?	Consolidated data
Yes, full responsibility	28%
Yes, some responsibility	58%
Yes, minimum responsibility	14%
No responsibility (Stop)	0%
Total	100%

Part 2. Attributions

Q1. Please rate each one of the following statements using the opinion scale from "strongly agree" to "strongly disagree" provided below each item.	
Q1a. My company is committed to cyber automation as part of its defense.	Consolidated data
Strongly agree	29%
Agree	32%
Unsure	15%
Disagree	18%
Strongly disagree	6%
Total	100%

Q1b. My company's leaders believe that smart machines will replace skilled security personnel.	Consolidated data
Strongly agree	20%
Agree	20%
Unsure	18%
Disagree	29%
Strongly disagree	13%
Total	100%

Q1c. My company's use of cyber automation will reduce operating costs.	Consolidated data
Strongly agree	26%
Agree	33%
Unsure	14%
Disagree	21%
Strongly disagree	6%
Total	100%

Q1d. My company's use of cyber automation will reduce personnel costs.	Consolidated data
Strongly agree	26%
Agree	29%
Unsure	16%
Disagree	22%
Strongly disagree	7%
Total	100%

Q1e. The inability to properly staff skilled security personnel has increased my company's investment in the automation of cyber tools and technologies.	Consolidated data
Strongly agree	26%
Agree	27%
Unsure	16%
Disagree	22%
Strongly disagree	8%
Total	100%

Q1f. My company's use of cyber automation will reduce the rate of false positives in the investigation of security alerts.	Consolidated data
Strongly agree	30%
Agree	32%
Unsure	15%
Disagree	16%
Strongly disagree	7%
Total	100%

Q1g. My company's migration to the cloud has increased the need for automation of cyber tools and technologies.	Consolidated data
Strongly agree	26%
Agree	33%
Unsure	15%
Disagree	20%
Strongly disagree	6%
Total	100%

Q1h. The integration of cybersecurity automation within my company's existing IT security architecture is a complex and time-consuming process.	Consolidated data
Strongly agree	28%
Agree	32%
Unsure	14%
Disagree	17%
Strongly disagree	9%
Total	100%

Q1i. Cyber automation will never fully replace human involvement and expertise.	Consolidated data
Strongly agree	36%
Agree	35%
Unsure	12%
Disagree	11%
Strongly disagree	6%
Total	100%

Part 3. Background

Q2. Using the following 10-point scale, please rate your organization's effectiveness in detecting cyber exploits, attacks or breaches?	Consolidated data
1 or 2	12%
3 or 4	15%
5 or 6	35%
7 or 8	24%
9 or 10	15%
Total	100%
Extrapolated value	5.84

Q3. Using the following 10-point scale, please rate your organization's effectiveness in minimizing false positives in the detection of cyber exploits, attacks or breaches?	Consolidated data
1 or 2	10%
3 or 4	12%
5 or 6	35%
7 or 8	24%
9 or 10	19%
Total	100%
Extrapolated value	6.11

Q4. Using the following 10-point scale, please rate your organization's effectiveness in minimizing the damages caused by cyber exploits, attacks or breaches?	Consolidated data
1 or 2	13%
3 or 4	17%
5 or 6	27%
7 or 8	26%
9 or 10	17%
Total	100%
Extrapolated value	5.82

Q5. Using the following 10-point scale, please rate your organization's effectiveness in prioritizing the cyber threats and vulnerabilities that pose the greatest risk?	Consolidated data
1 or 2	8%
3 or 4	14%
5 or 6	29%
7 or 8	29%
9 or 10	21%
Total	100%
Extrapolated value	6.32

Q6. Who in your organization is most responsible for ensuring a strong cybersecurity posture?	Consolidated data
CIO/CTO	29%
CISO/CSO	17%
Incident response team (CSIRT)	9%
Forensics team	5%
Lines of business	16%
Managed security service provider (MSSP)	6%
No one person or function	18%
Other (please specify)	0%
Total	100%

Q7. What best describes your organization's approach to cyber defense?	Consolidated data
Our approach primarily relies on automated tools (including machine learning and artificial intelligence)	20%
Our approach primarily relies on manual activities	34%
Our approach relies on a combination of automated tools and manual activities	22%
Our approach is "ad hoc" or is not specified	25%
Total	100%

Q8. In the typical week, how many malware alerts does your organization receive?	Consolidated data
Less than 50	8%
50 to 100	11%
101 to 1,000	18%
1,001 to 5,000	29%
5,001 to 10,000	16%
10,001 to 50,000	10%
50,001 to 100,000	4%
More than 100,000	3%
Total	100%
Extrapolated value	12,172

Q9. In your experience, what percent of these alerts are reliable?	Consolidated data
Less than 10%	35%
10% to 25%	40%
26% to 50%	14%
51% to 75%	7%
76% to 100%	3%
Total	100%
Extrapolated value	21%

Q10. What percent of these alerts pertains to advanced persistent threats?	Consolidated data
Less than 10%	34%
10% to 25%	39%
26% to 50%	20%
51% to 75%	6%
76% to 100%	1%
Total	100%
Extrapolated value	20%

Q11. What are the main intelligence sources used by your organization's cyber defense? Select your top two choices.	Consolidated data
Vendor-supplied information	77%
Peer-to-peer communications	60%
Intelligence sharing within industry group (ISAC)	35%
Information received from government	24%
Information received from law enforcement	4%
Other (please specify)	0%
Total	200%

Q12. In the typical week, how many cybersecurity alerts are actually investigated?	Consolidated data
Less than 5	16%
5 to 50	24%
51 to 100	17%
101 to 500	19%
501 to 1,000	15%
1,001 to 5,000	7%
5,001 to 10,000	1%
More than 10,000	0%
Total	100%
Extrapolated value	518

Q13. In the typical week, how many cyber exploits or malware infections go undetected (i.e., they bypass your organization's IPS and/or AV systems)? Please provide your best guess as a percentage of total cybersecurity alerts investigated estimated in Q12.	Consolidated data
Less than 1%	2%
1% to 10%	8%
11% to 20%	6%
21% to 30%	23%
31% to 40%	24%
41% to 50%	17%
Greater than 50%	20%
Total	100%
Extrapolated value	34%

Q14a. Does your organization have automated tools and/or technologies that capture intelligence and evaluate the true threat posed by cyber attackers?	Consolidated data
Yes	53%
No	47%
Total	100%

Q14b. What best describes the adequacy of automated tools and/or technologies deployed by your organization today?	Consolidated data
More than adequate	9%
Adequate	41%
Not adequate	29%
Inadequate	20%
Total	100%

Q14c. If yes, what percent of cyber exploits or malware containment can be handled by automated tools without requiring human intervention?	Consolidated data
Less than 10%	11%
10% to 25%	15%
26% to 50%	18%
51% to 75%	30%
76% to 100%	25%
Total	100%
Extrapolated value	51%

Q15. Within your organization, how many security staff members (i.e., personnel) are involved in the cyber exploit or malware containment process?	Consolidated data
1 to 5	1%
6 to 10	20%
11 to 15	29%
16 to 20	18%
21 to 25	17%
More than 25	14%
Total	100%
Extrapolated value	16.8

Q16. On average, how many years of professional experience do security staff members who handle malware containment have?	Consolidated data
1 to 3 years	12%
4 to 6 years	28%
7 to 9 years	34%
10 to 15 years	16%
More than 15 years	10%
Total	100%
Extrapolated value	8.5

Q17. How has the volume or frequency of cyber exploits changed over the past 12 months?	Consolidated data
Significant increase	14%
Increase	39%
Stayed the same	37%
Decrease	7%
Significant decrease	2%
Total	100%

Q18. How has the severity of cyber exploits changed over the past 12 months?	Consolidated data
Significant increase	19%
Increase	39%
Stayed the same	33%
Decrease	7%
Significant decrease	2%
Total	100%

Part 4. Estimating time containing cyber exploits

Q19. Approximately, how many hours each week is spent organizing and planning the organization's approaches to cyber defense? Please estimate the aggregate hours of the cybersecurity or InfoSec team.	
Q19a. Not facilitated by automation	Consolidated data
Less than 5	2%
5 to 10	23%
11 to 25	22%
26 to 50	9%
51 to 100	4%
101 to 250	2%
251 to 500	0%
More than 500	0%
Total	100%
Extrapolated value	16.6

Q19b. Facilitated by automation	Consolidated data
Less than 5	0%
5 to 10	32%
11 to 25	11%
26 to 50	8%
51 to 100	1%
101 to 250	1%
251 to 500	0%
More than 500	0%
Total	100%
Extrapolated value	9.7

Reduction in hours per week	6.9

Q20. Approximately, how many hours each week is spent capturing actionable intelligence about cyber exploits and malware infections? Please estimate the aggregate hours of the cybersecurity or InfoSec team.	
Q20a. Not facilitated by automation	Consolidated data
Less than 5	8%
5 to 10	14%
11 to 25	19%
26 to 50	26%
51 to 100	14%
101 to 250	8%
251 to 500	9%
More than 500	2%
Total	100%
Extrapolated value	73.2

Q20b. Facilitated by automation	Consolidated data
Less than 5	17%
5 to 10	18%
11 to 25	24%
26 to 50	18%
51 to 100	14%
101 to 250	9%
251 to 500	2%
More than 500	0%
Total	103%
Extrapolated value	36.4

Reduction in hours per week	36.7

Q21. Approximately, how many hours each week are spent evaluating actionable intelligence about cyber exploits or malware? Please estimate the aggregate hours of the cybersecurity or InfoSec team.	
Q21a. Not facilitated by automation	Consolidated data
Less than 5	1%
5 to 10	16%
11 to 25	22%
26 to 50	30%
51 to 100	16%
101 to 250	8%
251 to 500	4%
More than 500	1%
Total	97%
Extrapolated value	49.7

Q21b. Facilitated by automation	Consolidated data
Less than 5	22%
5 to 10	27%
11 to 25	30%
26 to 50	13%
51 to 100	7%
101 to 250	0%
251 to 500	0%
More than 500	0%
Total	100%
Extrapolated value	14.7

Reduction in hours per week	35.0

Q22. Approximately, how many hours each week are spent investigating actionable intelligence about cyber exploits or malware? Please estimate the aggregate hours of the cybersecurity or InfoSec team.	
Q22a. Not facilitated by automation	Consolidated data
Less than 5	2%
5 to 10	5%
11 to 25	8%
26 to 50	11%
51 to 100	23%
101 to 250	21%
251 to 500	21%
More than 500	9%
Total	100%
Extrapolated value	177.4

Q22b. Facilitated by automation	Consolidated data
Less than 5	1%
5 to 10	16%
11 to 25	21%
26 to 50	27%
51 to 100	18%
101 to 250	12%
251 to 500	5%
More than 500	0%
Total	100%
Extrapolated value	55.1

Reduction in hours per week	122.2

Q23. Approximately, how many hours each week are spent cleaning, fixing and/or patching networks, applications and devices (i.e., endpoints) damaged/infected by cyber exploits or malware? Please estimate the aggregate hours of the cybersecurity or InfoSec team.	
Q23a. Not facilitated by automation	Consolidated data
Less than 5	0%
5 to 10	1%
11 to 25	7%
26 to 50	14%
51 to 100	19%
101 to 250	29%
251 to 500	21%
More than 500	10%
Total	100%
Extrapolated value	195.2

Q23b. Facilitated by automation	Consolidated data
Less than 5	12%
5 to 10	16%
11 to 25	27%
26 to 50	28%
51 to 100	11%
101 to 250	3%
251 to 500	4%
More than 500	0%
Total	100%
Extrapolated value	36.9

Reduction in hours per week	158.2

Q24. Approximately, how many hours each week are spent documenting and/or reporting upon the cyber event (in conformance with policies or compliance mandates)? Please estimate the aggregate hours of the cybersecurity or InfoSec team.	
Q24a. Not facilitated by automation	Consolidated data
Less than 5	26%
5 to 10	48%
11 to 25	12%
26 to 50	8%
51 to 100	4%
101 to 250	2%
251 to 500	0%
More than 500	0%
Total	100%
Extrapolated value	14.0

Q24b. Facilitated by automation	Consolidated data
Less than 5	51%
5 to 10	34%
11 to 25	14%
26 to 50	2%
51 to 100	0%
101 to 250	0%
251 to 500	0%
More than 500	0%
Total	100%
Extrapolated value	6.9

Reduction in hours per week	7.1

Q25. Approximately, how much time is spent by security staff members are wasted because alerts they chase are erroneous (i.e., false positives)? Please estimate the aggregate hours of the cybersecurity or InfoSec team.	
Q25a. Not facilitated by automation	Consolidated data
Less than 5	0%
5 to 10	0%
11 to 25	3%
26 to 50	4%
51 to 100	8%
101 to 250	14%
251 to 500	34%
More than 500	39%
Total	103%
Extrapolated value	390.4

Q25b. Facilitated by automation	Consolidated data
Less than 5	8%
5 to 10	12%
11 to 25	22%
26 to 50	24%
51 to 100	21%
101 to 250	12%
251 to 500	0%
More than 500	0%
Total	100%
Extrapolated value	38.1

Reduction in hours per week	352.3

Q26. Approximately, how much IT downtime occurs each week because cyber attacks that resulted in a full or partial shutdown	
Q26a. Not facilitated by automation	Consolidated data
Less than 1	23%
1 to 2	34%
3 to 4	22%
5 to 6	13%
7 to 8	6%
9 to 10	2%
11 to 15	1%
More than 15	0%
Total	100%
Extrapolated value	2.8

Q26b. Facilitated by automation	Consolidated data
Less than 1	49%
1 to 2	46%
3 to 4	5%
5 to 6	0%
7 to 8	0%
9 to 10	0%
11 to 15	0%
More than 15	0%
Total	100%
Extrapolated value	1.1

Reduction in hours per week	1.7

Q27. What is the likelihood of a data breach involving 10,000 or more records containing sensitive or confidential personal information of customers or consumers (users) within the next 12 months? Your best guess is welcome.	
Q27a. Not facilitated by automation	Consolidated data
Zero	0%
1 to 2%	0%
2 to 4%	5%
5 to 7%	20%
8 to 10%	27%
11 to 15%	26%
16 to 25%	13%
More than 25%	9%
Total	100%
Extrapolated value	13.4%

Q27b. Facilitated by automation	Consolidated data
Zero	1%
1 to 2%	9%
2 to 4%	18%
5 to 7%	25%
8 to 10%	28%
11 to 15%	14%
16 to 25%	5%
More than 25%	0%
Total	100%
Extrapolated value	7.7%

Reduction in the likelihood of data breach over 12 months	5.7%

Part 5. Your role and organization

D1. What organizational level best describes your current position?	Consolidated data
Senior Executive/VP	6%
Director	14%
Manager	21%
Supervisor	17%
Technician	24%
Staff/Analyst	14%
Consultant	3%
Contractor	1%
Other	0%
Total	100%

D2. Check the primary person you or your IT security leader reports to within the organization.	Consolidated data
CEO/COO	1%
Chief Financial Officer	1%
General Counsel	1%
Chief Information Officer	57%
CISO/CSO	17%
Chief Compliance Officer	4%
Head, IT Operations	7%
General Manager (LOB)	6%
Chief Risk Officer	5%
Other	0%
Total	100%

D3. What industry best describes your organization's industry focus?	Consolidated data
Agriculture & food services	1%
Communications	3%
Consumer products	5%
Defense & aerospace	1%
Education & research	2%
Energy & utilities	6%
Entertainment & media	3%
Financial services	16%
Health & pharmaceuticals	9%
Hospitality	4%
Industrial & manufacturing	13%
Public sector	11%
Retail	8%
Services	9%
Technology & software	7%
Transportation	2%
Other	0%
Total	100%

D4. What is the worldwide headcount of your organization?	Consolidated data
Less than 500	11%
500 to 1,000	18%
1,001 to 5,000	22%
5,001 to 25,000	20%
25,001 to 50,000	19%
50,001 to 75,000	6%
More than 75,000	5%
Total	100%

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.

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.