The Cost of Malware Containment

Sponsored by

Damballa

Independently conducted by Ponemon Institute LLC

Publication Date: January 2015

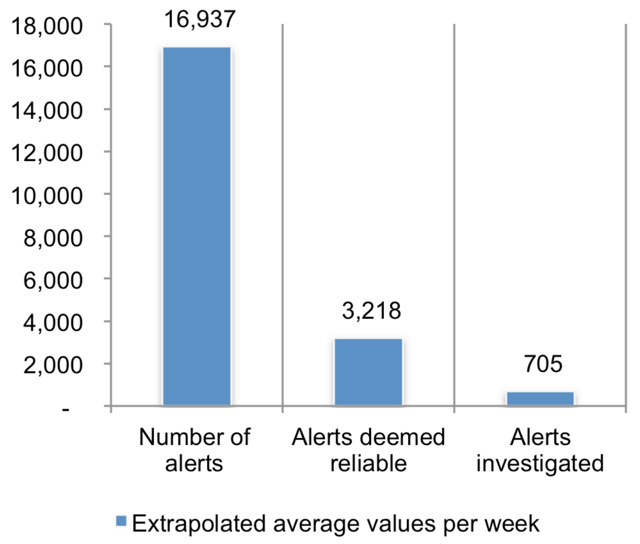
The Cost of Malware Containment

Ponemon Institute, January 2015

Part 1. Introduction

The recent Target, Home Depot, JPMorgan Chase and Sony Pictures Entertainment breaches are examples of how destructive malware can be to an organization's reputation and financial stability. Moreover, the severity and frequency of malware attacks has increased significantly in the past year, according to *The Cost of Malware Containment*, sponsored by Damballa.

Figure 1. Extrapolated average malware alerts for organizations participating in this study



Ponemon Institute conducted this research to understand how much money organizations are wasting in their efforts to prevent malware driven threats and other malicious programs from stealing high value and confidential data. To ensure a knowledgeable participant, we surveyed 630 IT and IT security practitioners in the United States who are familiar with their organization's practices for containing malware infections. They also have responsibility in detecting, evaluating and/or containing malware infections within their organization.

As noted in Figure 1, in a typical week an organization can receive an average of nearly 17,000 malware alerts. According to this research, the time to respond to these alerts is a severe drain on an organization's financial resources and IT security personnel. The average cost of time wasted responding to inaccurate and erroneous intelligence can average $1.27 million annually. Of all alerts, 19 percent (3,218) are considered reliable but only 4 percent (705) are investigated.

Following are the key findings:

Approximately 4 percent of all malware alerts are investigated. On average, organizations receive almost 17,000 malware alerts in a typical week but only 19 percent of these alerts are deemed to be reliable. Of the 3,218 reliable alerts, only 705 are investigated. This suggests that participating organizations do not have the resources or in-house expertise to detect or block serious malware.

Two-thirds of the time spent by security staff responding to malware alerts is wasted because of faulty intelligence. It costs organizations an average of $1.27 million annually in time wasted responding to erroneous or inaccurate malware alerts. According to respondents, an average of 395 hours is wasted each week detecting and containing malware because of false positives and/or false negatives. The extrapolated average value of lost time is estimated at approximately $25,000 per week or $1.27 million each year for participating organizations.

Malware infections have become more severe in the past year. Sixty percent of respondents say the severity of malware infections have significantly increased (16 percent) or increased (44 percent) in the past year. A smaller percentage (45 percent) of respondents say volume has increased in the past 12 months.

Many organizations have an unstructured or "ad hoc" approach to the malware containment process with no one person or function accountable. While 67 percent of respondents report they have some type of structured approach to malware containment, 33 percent have an "ad hoc" approach. Thirty percent say they have a structured approach that relies on manual activities and 24 percent say they primarily rely upon automated tools. When asked about responsibility for the malware containment process, 40 percent of respondents say there is no one person or function accountable for the containment of malware and 45 percent say the CISO is most responsible.

Intelligence about malware threats mainly comes from vendors and peers. Sixty-nine percent of respondents say vendor supplied information is their main source of intelligence about malware threats followed by 64 percent who say it is peer-to-peer communications. Government and law enforcement are rarely the source of intelligence.

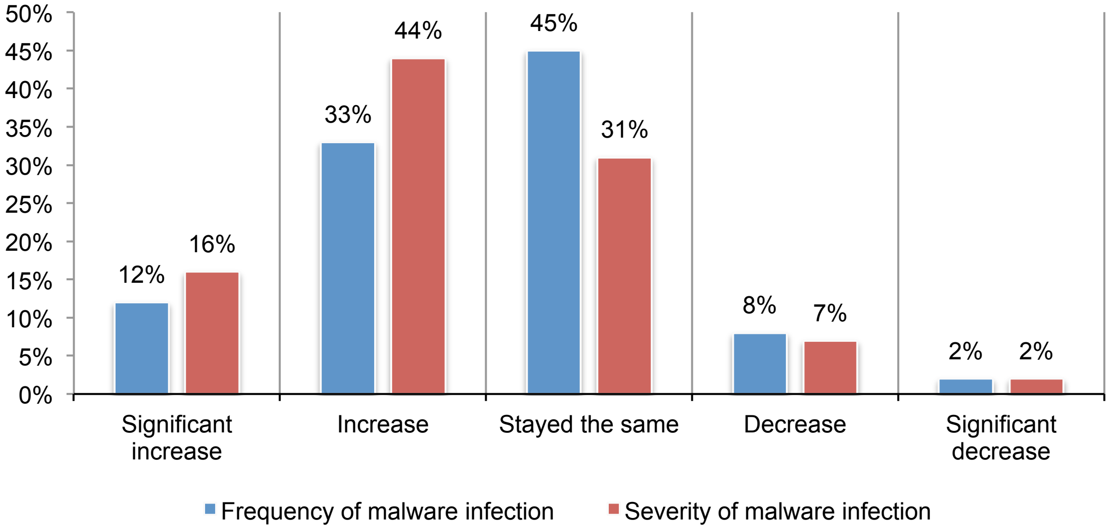
Most organizations do not have automated tools to capture intelligence and evaluate the true threat posed by malware. Only 41 percent of respondents say their organization has automated tools that capture intelligence and evaluate the true threat driven by malware. Organizations that have automated tools report that an average of 60 percent of malware containment does not require human input or intervention and can be handled by automated tools.

Part 2. Key findings

In this section, we provide a detailed analysis of the findings of this study. The complete audited findings are presented in the Appendix of this report.

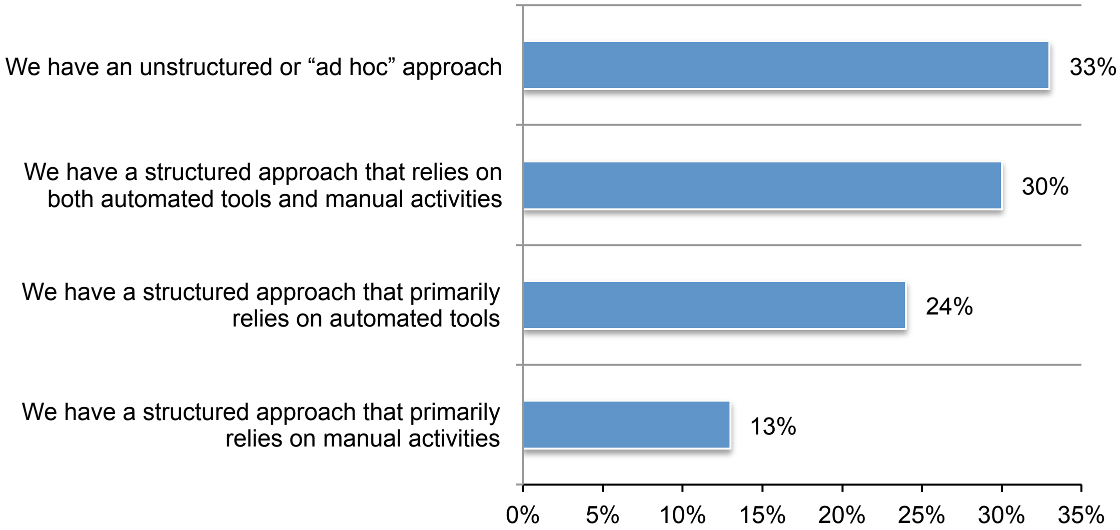
Malware infections have become more severe in the past year. According to Figure 2, 60 percent of respondents say the severity of malware infections have significantly increased (16 percent) or increased (44 percent) in the past year. A smaller percentage (45 percent) of respondents say volume has increased in the past 12 months.

Figure 2. Are malware infections increasing in volume and severity?



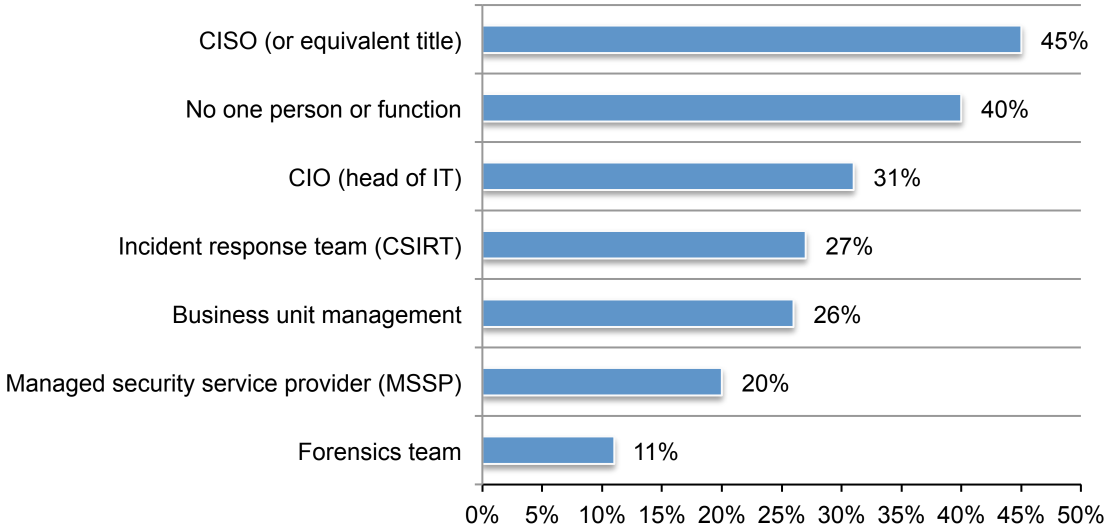
Many organizations have an unstructured or "ad hoc" approach to the malware containment process with no one person or function accountable. Figure 3 reveals that while 67 percent of respondents report they have some type of structured approach to malware containment, 33 percent have an "ad hoc" approach. Thirty percent say they have a structured approach that relies on both automated tools and manual activities and 24 percent say they primarily rely upon automated tools.

Figure 3. What is your organization's approach to malware containment?



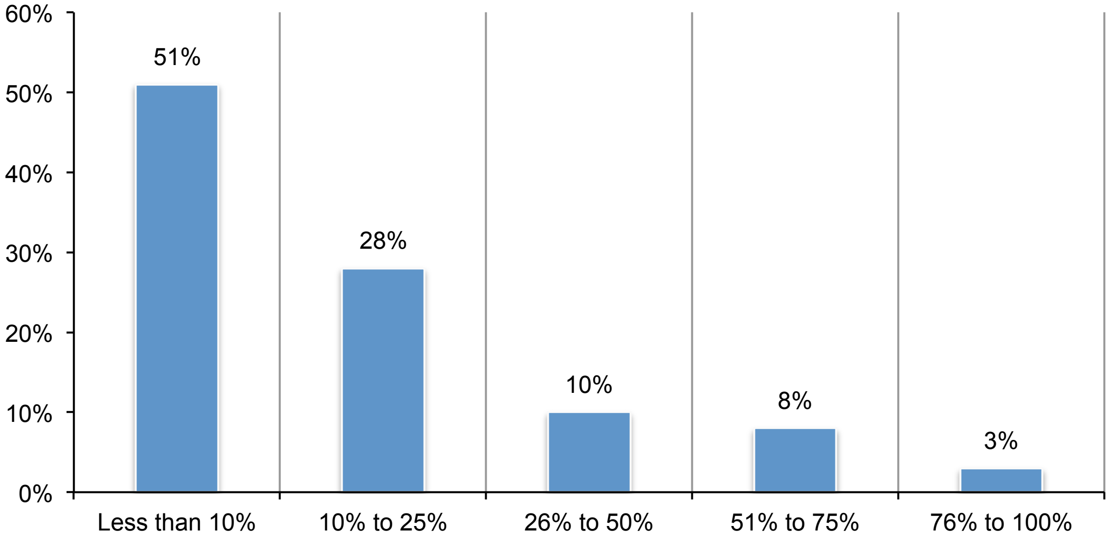
When asked about responsibility for the malware containment process, 40 percent of respondents also say there is no one person or function accountable for the containment of malware, as shown in Figure 4. Forty-five percent of respondents say the CISO is most responsible. The typical organization has 17 IT or IT security staff members involved in the malware detection and containment process. On average they have 8 years professional experience.

Figure 4. Who is responsible for the containment of malware?
Two responses permitted



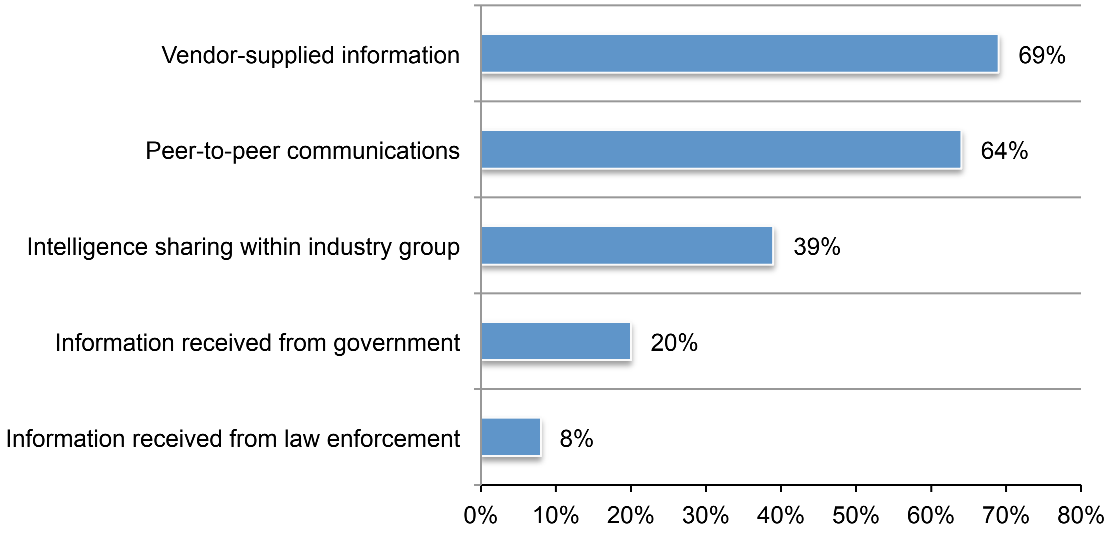
Approximately 4 percent of all malware alerts are investigated. On average, organizations receive almost 17,000 malware alerts in a typical week but only 19 percent of these alerts are deemed to be reliable, as shown in Figure 5. Of the 3,218 reliable alerts, only 705 are investigated. This suggests that participating organizations do not have the resources or in-house expertise to detect or block serious malware. On average, 42 percent of these alerts pertain to advanced malware threats.

Figure 5. Percentage of malware alerts that are deemed to be reliable
Extrapolated value = 19 percent



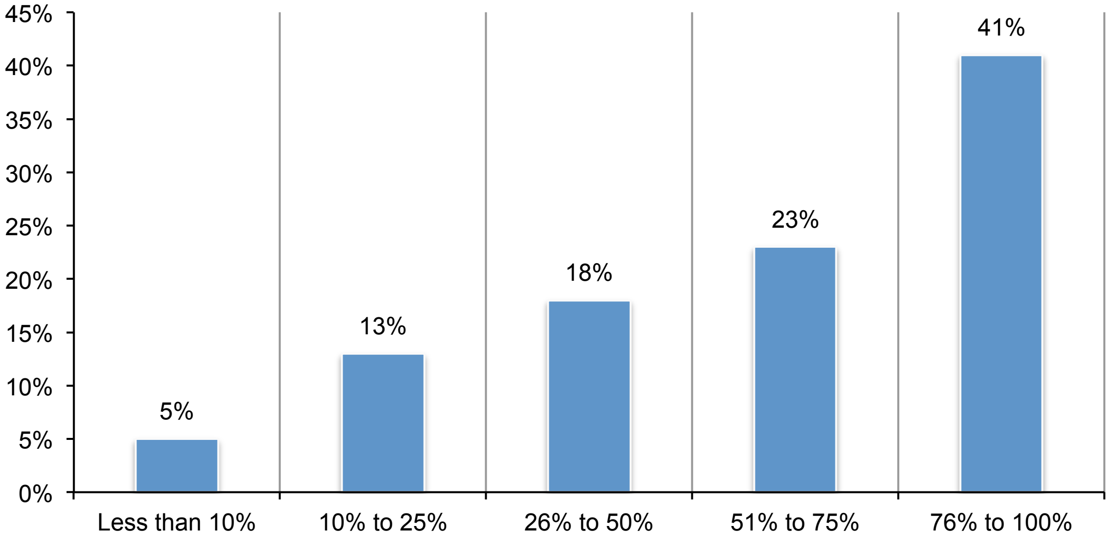
Intelligence about malware threats mainly comes from vendors and peers. According to Figure 6, 69 percent of respondents say vendor supplied information is their main source of intelligence about malware threats followed by 64 percent who say it is peer-to-peer communications. Government and law enforcement are rarely the source of intelligence.

Figure 6. Main malware intelligence sources used by organizations
Two responses permitted



Most organizations do not have automated tools to capture intelligence and evaluate the true threat posed by malware. Only 41 percent of respondents, say their organization has automated tools that capture intelligence and evaluate the true threat caused by malware. Organizations that have automated tools report that an average of 60 percent of malware containment does not require human input or intervention and can be handled by automated tools, as shown in Figure 7.

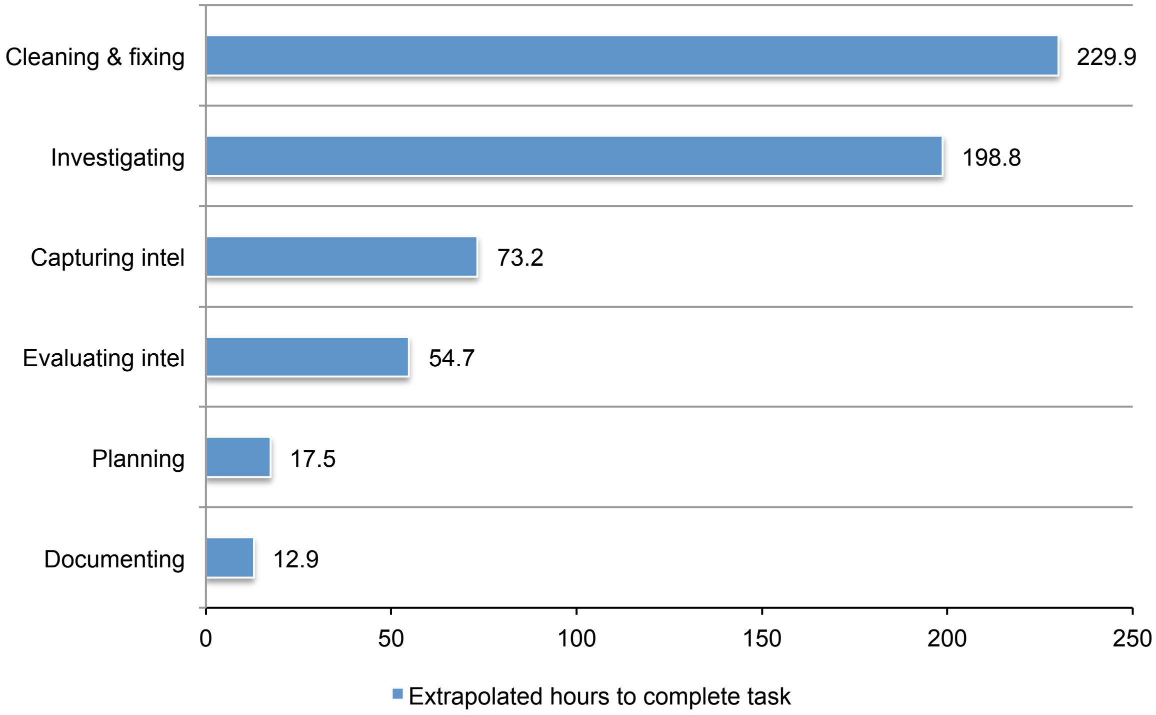
Figure 7. Percentage of malware containment that can be handled by automated tools
Extrapolated value = 60 percent



An average of almost 600 hours are spent each week on malware containment. To determine the amount of hours spent each week on malware containment, we asked respondents to estimate the time spent on the following activities shown in Figure 8.

The most time is spent cleaning and fixing and/or patching networks, applications and devices (i.e. endpoints) damaged or infected by malware (229.9 hours) and investigating actionable intelligence (198.8 hours). This is followed by capturing actionable intelligence (73.2 hours), evaluating actionable intelligence (54.7), organizing and planning approaches to malware detection, evaluation and containment (17.5 hours) and documenting and/or reporting upon the malware containment process (in conformance with policies or compliance mandates) (12.9 hours).

Figure 8. Estimated average hours spent to contain advanced malware
Total extrapolated average = 587 hours



It costs organizations an average of $1.27 million per annum or approximately $25,000 per week in time wasted responding to erroneous malware alerts. More than half of the time spent by security staff members investigating malware alerts is wasted because of inaccurate or erroneous intelligence. Accordingly, an average of 395 hours is wasted each week chasing false negatives and/or false positives. Table 1 shows the calculus used to estimate an average annual cost of $1.27 million each year or $25,000 each week for organizations participating in this study.

Table 1. Annual cost of the time wasted on malware containment	**Calculus**
Extrapolated hours per week	395
Extrapolated hours per year	20,533
Fully loaded wage rate*	$62.00
Extrapolated cost per year	$1,273,061

*The fully loaded wage hourly rate of supervisory level IT security practitioners in the US-based organizations is derived from Ponemon Institute's 2014 IT Security Spending Tracking Study.

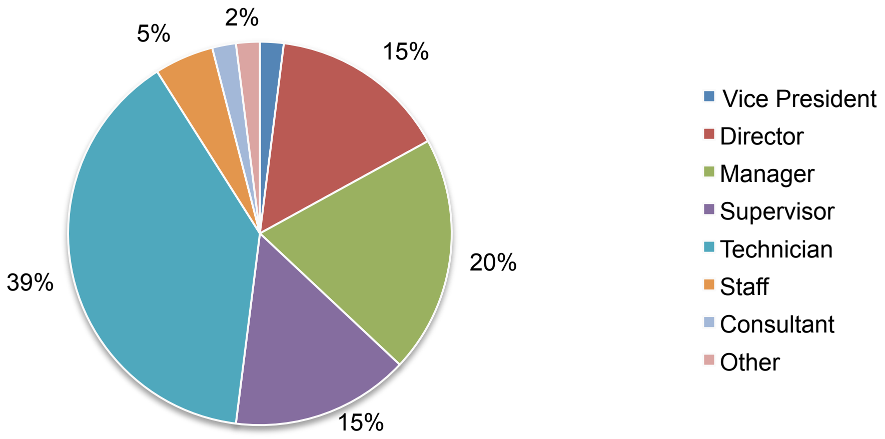
Part 3. Methods

A sampling frame composed of 18,750 IT and IT security practitioners located in the United States and who are familiar with their organization's practices for containing malware infections and have responsibility in detecting, evaluating and/or containing malware infections within their organization were selected for participation in this survey. As shown in Table 2, 706 respondents completed the survey. Screening removed 76 surveys. The final sample was 630 surveys (or a 3.4 percent response rate).

Table 2. Sample response	Freq	Pct%
Total sampling frame	18,750	100.0%
Total returns	706	3.8%
Rejected or screened surveys	76	0.4%
Final sample	630	3.4%

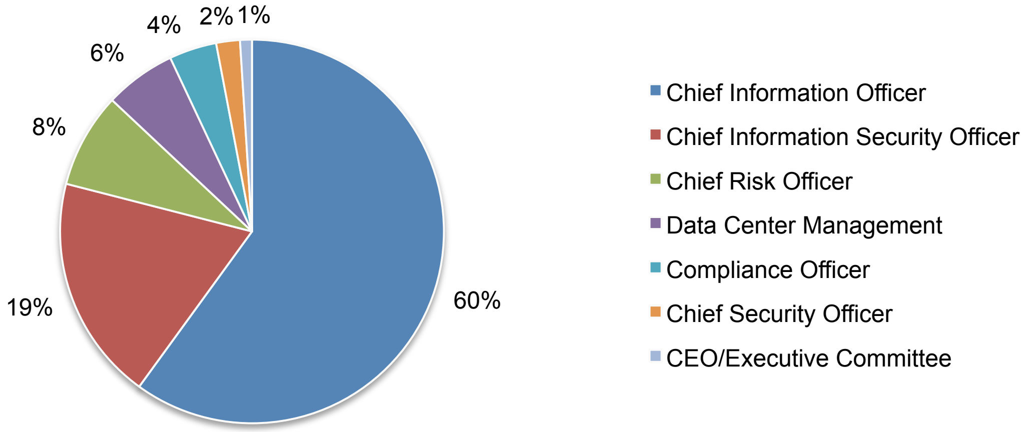
Pie chart 1 reports the current position or organizational level of the respondents. As shown in Pie Chart 1, more than half of respondents (52 percent) reported their position as supervisory or above.

Pie Chart 1. Current position or organizational level



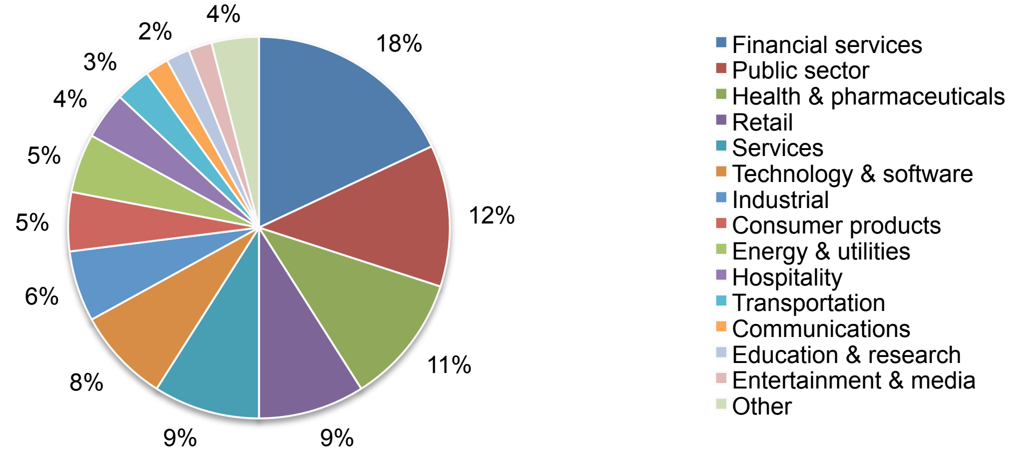
Pie Chart 2 identifies the primary person the respondent or their IT security leader reports to. Sixty percent of respondents identified the chief information officer and 19 percent reports to the chief information security officer.

Pie Chart 2. Primary person respondent or IT security leader reports to



Pie Chart 3 reports the primary industry classification of respondents' organizations. This chart identifies financial services (18 percent) as the largest segment, followed by public sector (12 percent) and health & pharmaceutical (11 percent).

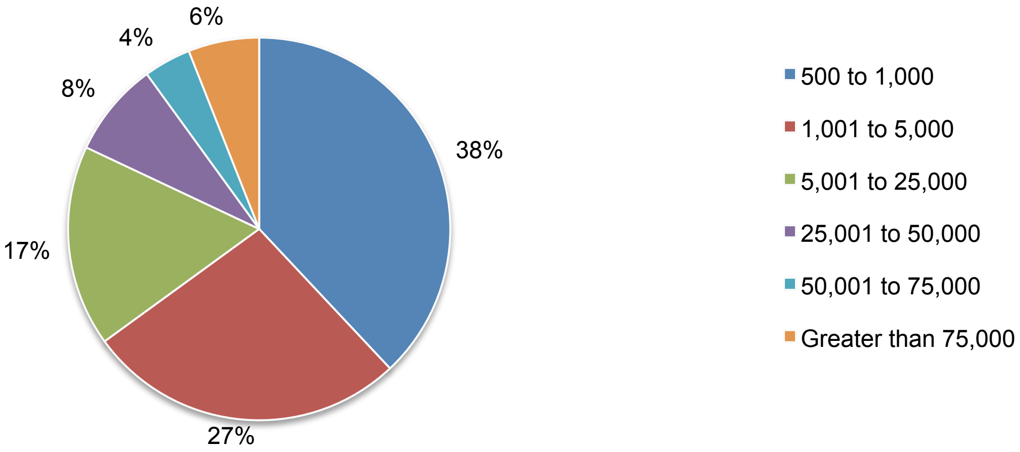
Pie Chart 3. Organizations industry classification



According to Pie Chart 4, more than half of the respondents (65 percent) are from organizations with a global headcount of less than 5,000 employees.

Pie Chart 4. Worldwide headcount of the organization

Extrapolated value = 13,945



Part 4. Caveats

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 in various organizations in the United States. 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 in November 2014.

Survey response	Freq	Pct%
Total sampling frame	18750	100.0%
Total returns	706	3.8%
Rejected or screened surveys	76	0.4%
Total sample	630	3.4%

Part 1. Screening questions

S1. How familiar are you with your organization's practices for containing malware infections?	Pct%
Very familiar	51%
Familiar	30%
Somewhat familiar	19%
No knowledge (Stop)	0%
Total	100%

S2. Do you have any responsibility in detecting, evaluating and/or containing malware infections within your organization?	Pct%
Yes, full responsibility	36%
Yes, some responsibility	49%
Yes, minimum responsibility	15%
No responsibility (Stop)	0%
Total	100%

Part 2. Background

Q1. Using the following 10-point scale, please rate your organization's effectiveness in detecting malware infections?	Pct%
1 or 2	9%
3 or 4	10%
5 or 6	27%
7 or 8	35%
9 or 10	19%
Total	100%
Extrapolated value	6.40

Q2. Using the following 10-point scale, please rate your organization's effectiveness in minimizing false positives in the detection of malware infections?	Pct%
1 or 2	18%
3 or 4	19%
5 or 6	32%
7 or 8	23%
9 or 10	8%
Total	100%
Extrapolated value	5.18

Q3. Using the following 10-point scale, please rate your organization's effectiveness in minimizing the damages caused by actual malware infections?	Pct%
1 or 2	20%
3 or 4	20%
5 or 6	31%
7 or 8	22%
9 or 10	7%
Total	100%
Extrapolated value	5.02

Q4. Using the following 10-point scale, please rate your organization's effectiveness in prioritizing the malware infections that pose the greatest risk?	Pct%
1 or 2	15%
3 or 4	22%
5 or 6	29%
7 or 8	25%
9 or 10	9%
Total	100%
Extrapolated value	5.32

Q5. Who in your organization is most responsible for the containment of malware? Select the top two choices.	Pct%
CIO (head of IT)	31%
CISO (or equivalent title)	45%
Incident response team (CSIRT)	27%
Forensics team	11%
Business unit management	26%
Managed security service provider (MSSP)	20%
No one person or function	40%
Other (please specify)	0%
Total	200%

Q6. What best describes your organization's malware containment process?	Pct%
We have a structured approach that primarily relies on automated tools	24%
We have a structured approach that primarily relies on manual activities	13%
We have a structured approach that relies on both automated tools and manual activities	30%
We have an unstructured or "ad hoc" approach	33%
Total	100%

Q7. In the typical week, how many malware alerts does your organization receive?	Pct%
Less than 50	10%
50 to 100	5%
101 to 1,000	21%
1,001 to 5,000	23%
5,001 to 10,000	19%
10,001 to 50,000	9%
50,001 to 100,000	8%
More than 100,000	5%
Total	100%
Extrapolated value	16,937

Q8. In your experience, what percent of these alerts are reliable?	Pct%
Less than 10%	51%
10% to 25%	28%
26% to 50%	10%
51% to 75%	8%
76% to 100%	3%
Total	100%
Extrapolated value	19%

Q9. What percent of these alerts pertains to advanced malware threats?	Pct%
Less than 10%	30%
10% to 25%	15%
26% to 50%	8%
51% to 75%	24%
76% to 100%	23%
Total	100%
Extrapolated value	42%

Q10. What are the main intelligence sources about malware used by your organization? Select your top two choices.	Pct%
Vendor-supplied information	69%
Peer-to-peer communications	64%
Intelligence sharing within industry group	39%
Information received from government	20%
Information received from law enforcement	8%
Other (please specify)	0%
Total	200%

Q11. In the typical week, how many malware alerts are actually investigated?	Pct%
Less than 5	14%
5 to 50	15%
51 to 100	33%
101 to 500	17%
501 to 1,000	9%
1,001 to 5,000	9%
5,001 to 10,000	2%
More than 10,000	1%
Total	100%
Extrapolated value	704.8

Q12. In the typical week, how many 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 malware infections investigated/estimated in Q11.	Pct%
Less than 1%	6%
1% to 10%	4%
11% to 20%	8%
21% to 30%	12%
31% to 40%	13%
41% to 50%	23%
Greater than 50%	34%
Total	100%
Extrapolated value	40%

Q13a. Does your organization have automated tools that capture intelligence and evaluate the true threat posed by malware?	Pct%
Yes	41%
No	59%
Total	100%

Q13b. If yes, what percent of malware containment can be handled by automated tools without requiring human input or intervention?	Pct%
Less than 10%	5%
10% to 25%	13%
26% to 50%	18%
51% to 75%	23%
76% to 100%	41%
Total	100%
Extrapolated value	60%

Q14. Within your organization, how many security or IT staff members (i.e., personnel) are involved in the malware detection and containment process?	Pct%
1 to 5	10%
6 to 10	12%
11 to 15	13%
16 to 20	23%
21 to 25	32%
More than 25	10%
Total	100%
Extrapolated value	17.1

Q15. On average, how many years of professional experience do security staff members who handle malware containment have?	Pct%
1 to 3 years	8%
4 to 6 years	30%
7 to 9 years	39%
10 to 15 years	15%
More than 15 years	8%
Total	100%
Extrapolated value	7.9

Q16. In your opinion, how has the volume or frequency of malware infection changed over the past 12 months?	Pct%
Significant increase	12%
Increase	33%
Stayed the same	45%
Decrease	8%
Significant decrease	2%
Total	100%

Q17. In your opinion, how has the severity of malware infection changed over the past 12 months?	Pct%
Significant increase	16%
Increase	44%
Stayed the same	31%
Decrease	7%
Significant decrease	2%
Total	100%

Part 3. Estimating time to contain malware

Q18. Approximately, how many hours each week is spent organizing and planning the organization's approaches to malware detection, evaluation and containment? Please estimate the aggregate hours of the malware containment team.	Pct%
Less than 5	48%
5 to 10	25%
11 to 25	12%
26 to 50	10%
51 to 100	3%
101 to 250	1%
251 to 500	1%
More than 500	0%
Total	100%
Extrapolated value	17.5

Q19. Approximately, how many hours each week is spent capturing actionable intelligence about malware? Please estimate the aggregate hours of the malware containment team.	Pct%
Less than 5	9%
5 to 10	13%
11 to 25	15%
26 to 50	32%
51 to 100	15%
101 to 250	8%
251 to 500	7%
More than 500	1%
Total	100%
Extrapolated value	73.2

Q20. Approximately, how many hours each week are spent evaluating actionable intelligence about malware? Please estimate the aggregate hours of the malware containment team.	Pct%
Less than 5	0%
5 to 10	19%
11 to 25	30%
26 to 50	28%
51 to 100	11%
101 to 250	8%
251 to 500	4%
More than 500	0%
Total	100%
Extrapolated value	54.7

Q21. Approximately, how many hours each week are spent investigating actionable intelligence about malware? Please estimate the aggregate hours of the malware containment team.	Pct%
Less than 5	0%
5 to 10	6%
11 to 25	8%
26 to 50	15%
51 to 100	15%
101 to 250	22%
251 to 500	26%
More than 500	8%
Total	100%
Extrapolated value	198.8

Q22. Approximately, how many hours each week are spent cleaning, fixing and/or patching networks, applications and devices (i.e., endpoints) damaged/infected by malware? Please estimate the aggregate hours of the malware containment team.	Pct%
Less than 5	0%
5 to 10	3%
11 to 25	5%
26 to 50	6%
51 to 100	19%
101 to 250	30%
251 to 500	25%
More than 500	12%
Total	100%
Extrapolated value	229.9

Q23. Approximately, how many hours each week are spent documenting and/or reporting upon the malware containment process (in conformance with policies or compliance mandates)? Please estimate the aggregate hours of the malware containment team.	Pct%
Less than 5	27%
5 to 10	50%
11 to 25	11%
26 to 50	8%
51 to 100	4%
101 to 250	0%
251 to 500	0%
More than 500	0%
Total	100%
Extrapolated value	12.9

Recap	**Hours**
Planning	17.5
Capturing intel	73.2
Evaluating intel	54.7
Investigating	198.8
Cleaning & fixing	229.9
Documenting	12.9
Total hours per week	587.0

Q24. Approximately, what percent of time spent by security staff members are wasted because the malware alerts they chase are erroneous (i.e., false positives)? Please estimate the aggregate hours of the malware containment team.	Pct%
Less than 10%	2%
10% to 25%	5%
26% to 50%	14%
51% to 75%	32%
76% to 100%	47%
Total	100%
Extrapolated value	67%
Extrapolated hours of wasted time	395

Q25. Approximately, how much IT downtime occurs each week as a result of cleaning, fixing and/or patching of malware-infected networks, applications and devices? Please estimate the aggregate hours of unplanned downtime (including partial downtime).	Pct%
Less than 1	44%
1 to 2	29%
3 to 4	8%
5 to 6	7%
7 to 8	8%
9 to 10	2%
11 to 15	2%
More than 15	0%
Total	100%
Extrapolated value	2.5

Value of wasted time	Amount
Hours per week	395
Hours per year	20,533
Fully loaded wage rate	$62.00
Extrapolated cost per year	$1,273,061

Part 4. Your role and organization

D1. What organizational level best describes your current position?	Pct%
Senior Executive	1%
Vice President	2%
Director	15%
Manager	20%
Supervisor	15%
Technician	39%
Staff	5%
Consultant	2%
Contractor	1%
Other	0%
Total	100%

D2. Check the **Primary Person** you or your IT security leader reports to within the organization.	Pct%
CEO/Executive Committee	1%
Chief Financial Officer	0%
General Counsel	0%
Chief Information Officer	60%
Chief Information Security Officer	19%
Compliance Officer	4%
Human Resources VP	0%
Chief Security Officer	2%
Data Center Management	6%
Chief Risk Officer	8%
Other	0%
Total	100%

D3. What best describes your organization's industry classification?	Pct%
Agriculture & food services	1%
Communications	2%
Consumer products	5%
Defense & aerospace	1%
Education & research	2%
Energy & utilities	5%
Entertainment & media	2%
Financial services	18%
Health & pharmaceuticals	11%
Hospitality	4%
Industrial	6%
Public sector	12%
Retail	9%
Services	9%
Technology & software	8%
Transportation	3%
Other	2%
Total	100%

D4. What is the worldwide headcount of your organization?	Pct%
Less than 500 (stop)	0%
500 to 1,000	38%
1,001 to 5,000	27%
5,001 to 25,000	17%
25,001 to 50,000	8%
50,001 to 75,000	4%
Greater than 75,000	6%
Total	100%
Extrapolated value	13,945

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.