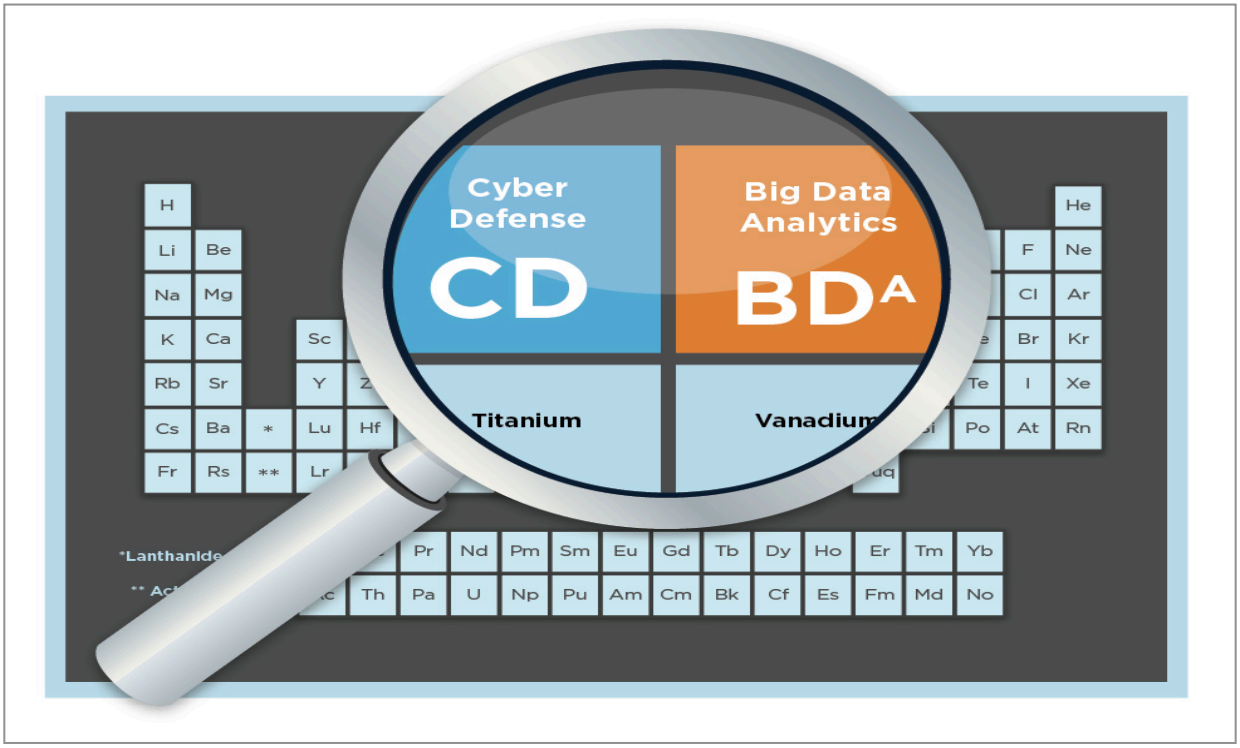


Big Data Analytics in Cyber Defense

Sponsored by Teradata

Independently conducted by Ponemon Institute LLC

Publication Date: February 2013

Big Data Analytics in Cyber Defense

Ponemon Institute, February 2013

Part 1. Introduction

Cyber attacks involve advanced and sophisticated techniques to infiltrate corporate networks and enterprise systems. Types of attacks include advanced malware, zero day attacks and advanced persistent threats. Advance warning about attackers and intelligence about the threat landscape is considered by many security leaders to be essential features in security technologies.[1]

The purpose of the *Big Data Analytics in Cyber Defense* study sponsored by Teradata and conducted by Ponemon Institute is to learn about organizations' cyber security defenses and the use of big data analytics[2] to become more efficient in recognizing the patterns that represent network threats. Big data analytics in security involves the ability to gather massive amounts of digital information to analyze, visualize and draw insights that can make it possible to predict and stop cyber attacks. The study looks at the awareness among IT and IT security practitioners about the new data management and analytic technologies now available to help organizations become more proactive and intelligent about detecting and stopping threats.

> Imagine the following scenario:
>
> Using big data analytics, you spot the formation of a distributed denial of service attack minutes before it hits your company's layered network defenses.
>
> You identify and contain the exfiltration of corporate secrets by malicious insiders, who are members of a criminal syndicate, located in an off shore data center. in another country.

In this study, we surveyed 706 IT and IT security practitioners in financial services, manufacturing and government with an average of 10 years experience. All respondents are familiar with their organization's defense against cyber security attacks and have some level of responsibility for managing the cyber security activities within their organization.

Following are noteworthy findings from this research:

- Cyber attacks are getting worse but only 20 percent say their organizations are more effective at stopping them. Greatest areas of cyber security risk are caused by mobility, lack of visibility and multiple global interconnected network systems.
- Less than half of organizations are vigilant in preventing (42 percent) anomalous and potentially malicious traffic from entering networks or detecting such traffic (49 percent) in their networks.
- Fifty-six percent are aware of the technologies that provide big data analytics and 61 percent say they will solve pressing security issues but only 35 percent have them. The outlook is good because 61 percent say big data analytics is in their future.
- Big data analytics + security technologies = stronger cyber defense posture. Eighty-two percent would like big data analytics combined with anti-virus/anti-malware and 80 percent say anti-DoS/DDoS would make their organizations more secure.

---

[1] Narus Validation Study, Ponemon Institute, November 2, 2010

[2] Big data analytics is defined as enabling organizations to discover previously unseen patterns and to develop actionable insights about their businesses and environments, including cyber defense. Cyber analytics applies big data tools and techniques to capture, process and refine network activity data, applies algorithms for near-real-time review of every network node and employs visualization tools to easily identify anomalous behavior required for fast response or investigation. Cyber analytics tools allow SOCs/NOCs and network analysts to more easily recognize patterns of activity that represent network threats.

Part 2. Key Findings

We organized this research according to the following topics:

- Perceptions about cyber readiness
- Cyber security risks, vulnerabilities and consequences
- Big data analytics & cyber security solutions
- Industry differences

Perceptions about organization's cyber readiness

Big data analytics can solve pressing security issues faced by companies and government, according to 61 percent of respondents. However, only 35 percent say they have solutions in place that are the same or comparable to big data analytics for cyber defense.

As shown in Figure 1, the majority of respondents (60 percent) agree that launching a strong defense against hackers and other cyber criminals requires their organization to see and quickly contain anomalous and potentially malicious traffic in networks. What is hindering organizations is the dearth of in-house personnel or expertise to analyze anomalous and potentially malicious traffic in networks, according to about half (51 percent) of respondents.

The majority of respondents in this study who are in IT and IT security see the value of big data analytics in addressing cyber risk. However, there is a significant difference in how the value is perceived by others in the organization. Less than half (47 percent) of respondents believe their organization considers big data analytics in cyber defense as very important. This suggests why creating awareness of the capability of these solutions is important.

Figure 1: Perceptions about cyber readiness
Strongly agree and agree response combined

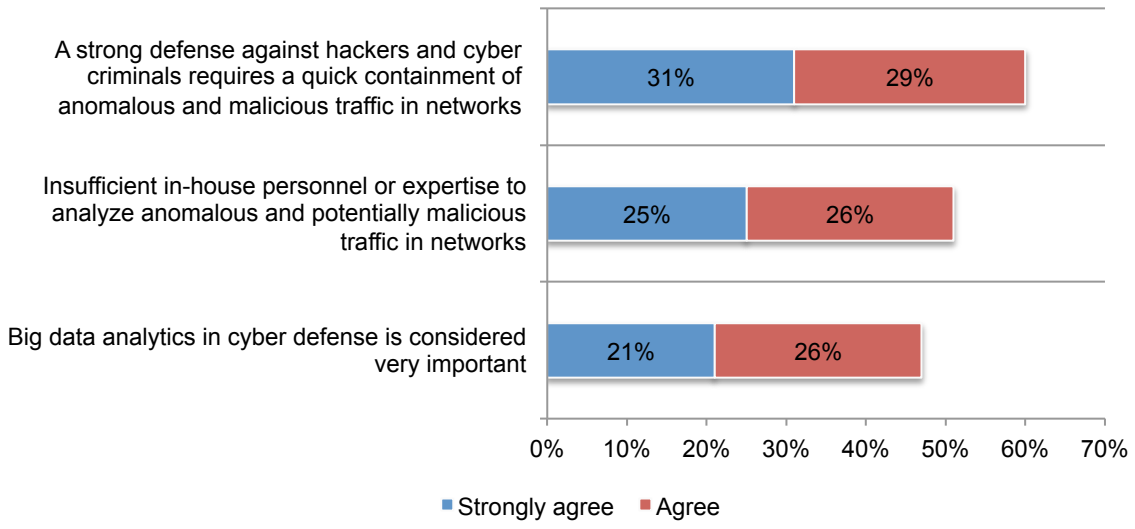
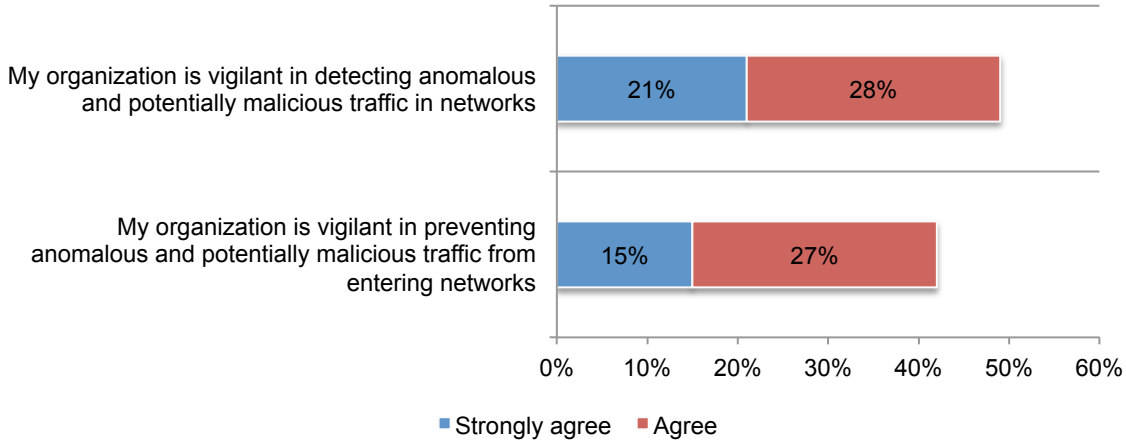


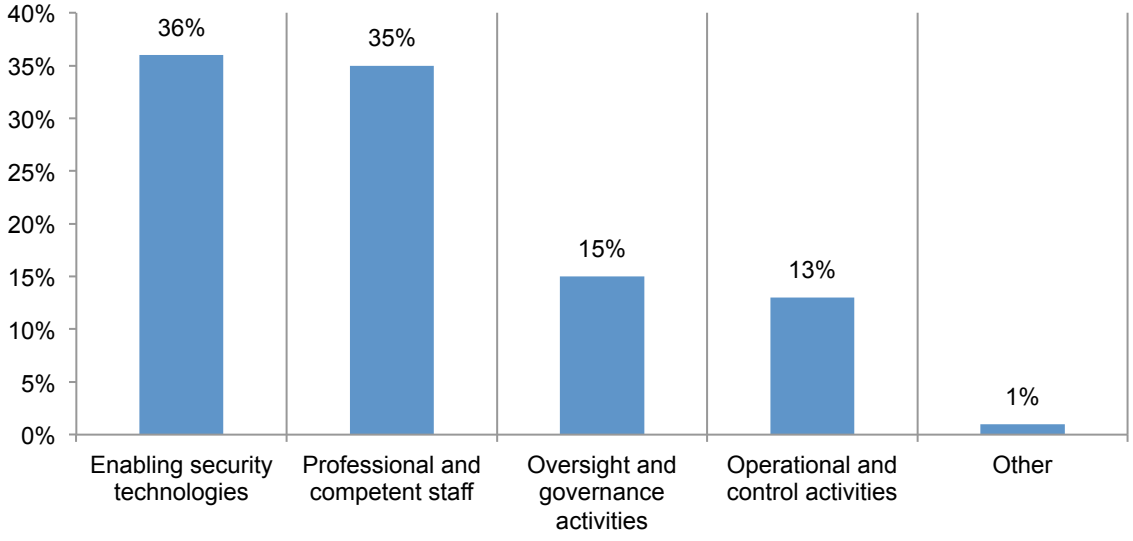
Figure 2 shows that less than half (49 percent) agree that their organization is vigilant in **detecting** anomalous and potentially malicious traffic from entering networks and a smaller percentage (42 percent) agree that their organization is vigilant in **preventing** such traffic.

Figure 2: Perceptions about prevention & detection of anomalous & malicious traffic
Strongly agree and agree response combined



When asked specifically where their organizations are most deficient in being able to become more proactive in their approach to cyber threats, 36 percent say it is enabling security technologies and 35 percent say it is professional expertise, as shown in Figure 3. Of less concern or perceived not to be deficient are oversight and governance activities and operational and control activities.

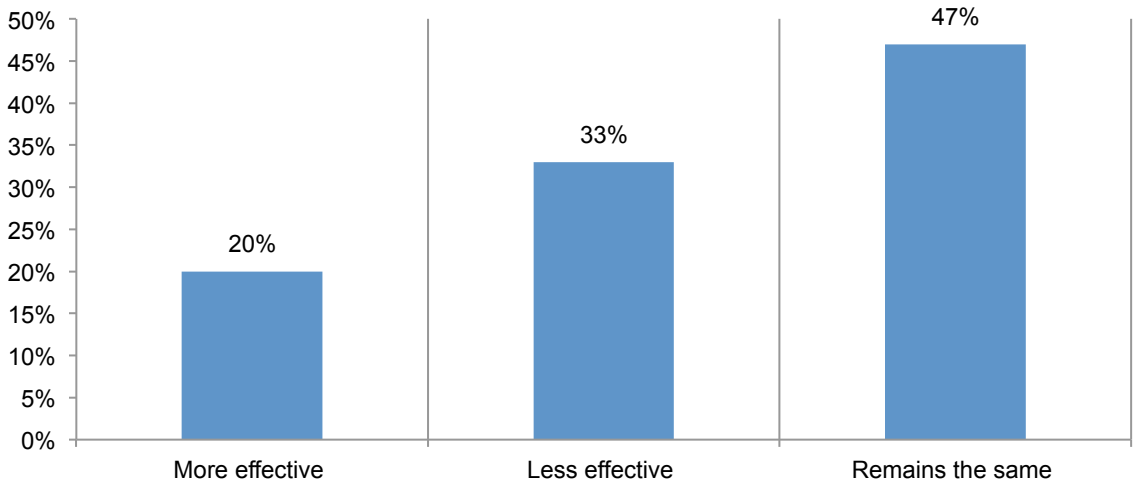
Figure 3: Deficiencies in cyber readiness



Cyber Security Risks, Consequences and Barriers to Improvement

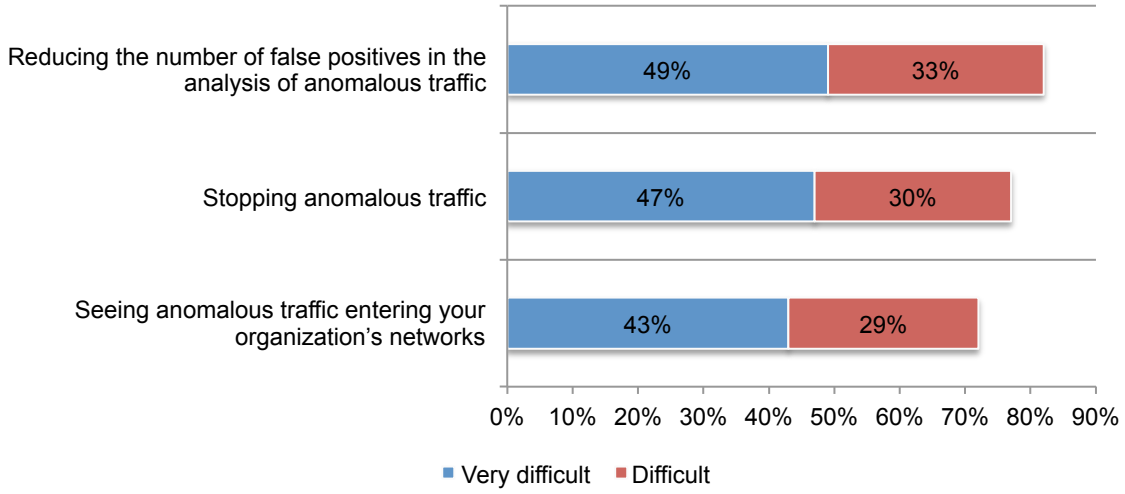
Figure 4 reveals that most organizations represented in this research are not achieving a more effective security posture in combating cyber attacks and intrusions. Thirty-three percent say their organization is less effective and 47 percent say their security posture is the same in terms of effectiveness.

Figure 4: The cyber security posture over the past 12 months



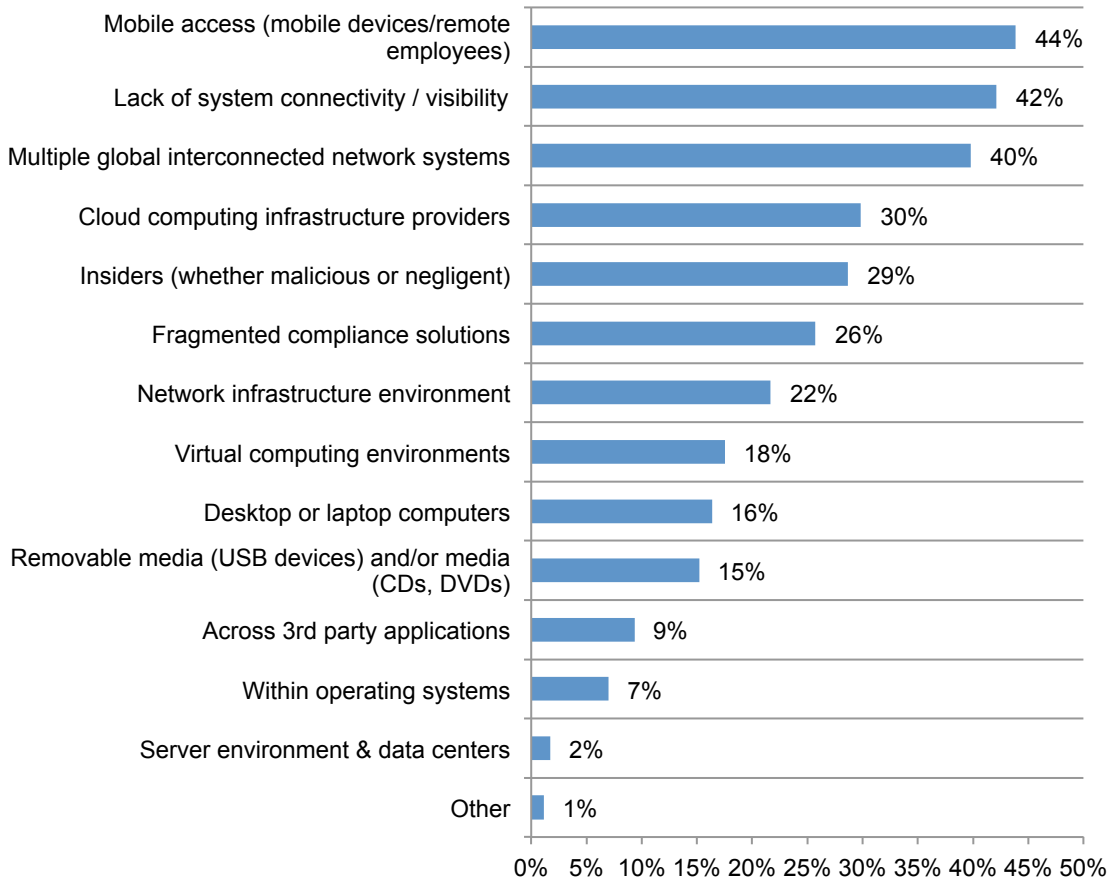
The most difficult for the IT respondents surveyed is the ability to reduce the number of false positives in the analysis of anomalous traffic. This is followed by the difficulty in stopping anomalous traffic and the difficulty in seeing anomalous traffic entering their networks as shown in Figure 5.

Figure 5: Difficulties with anomalous traffic
Very difficult and difficult response combined



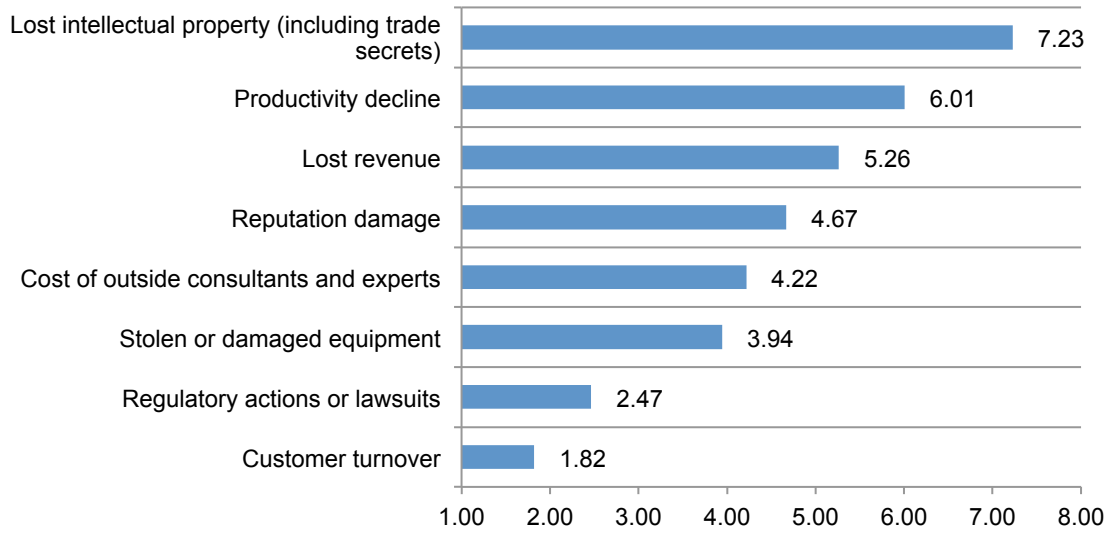
According to Figure 6, the greatest areas of cyber security risk are mobile access (either through mobile devices such as smart phones and mobile/remote employees), lack of system connectivity/visibility and multiple global interconnected network systems.

Figure 6: Greatest areas of potential cyber security risk within IT
Three choices permitted



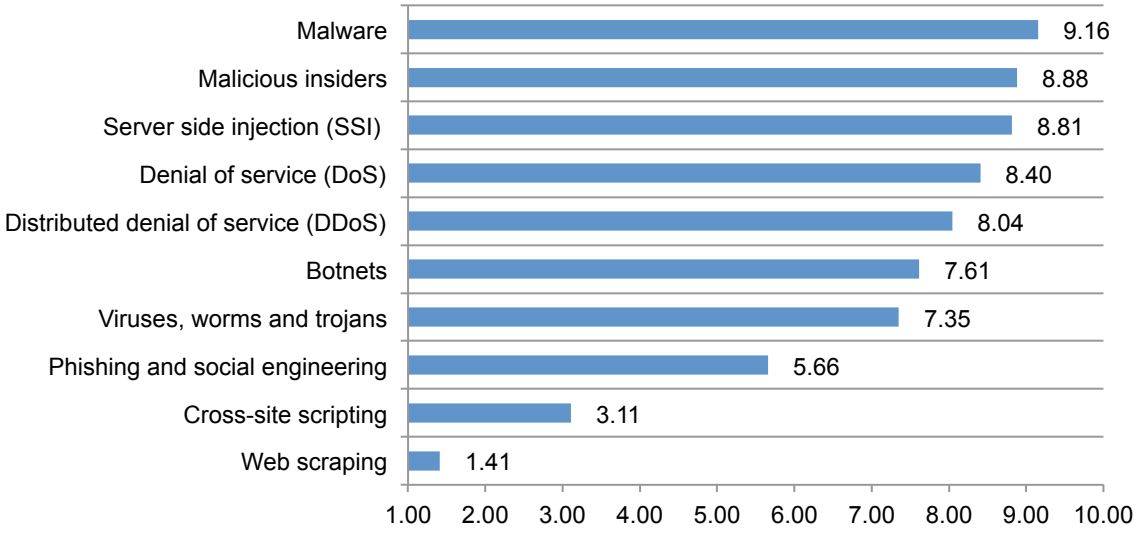
Theft of information assets, disruption of services and wrongful disclosure are believed to be the most serious cyber security threats to an organization's information assets. The most serious consequences from a cyber attack or intrusion are the loss of intellectual property, productivity decline and lost revenue, according to Figure 7.

Figure 7: Negative consequences resulting from a cyber attack or intrusion
8 = most severe to 1 = least severe (converted scale)



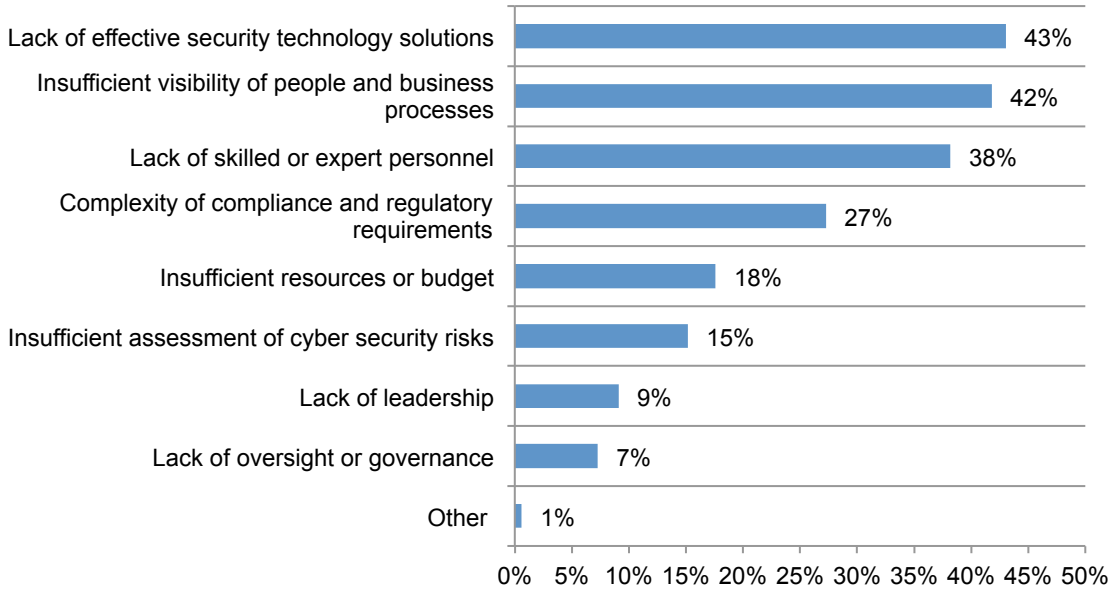
To reduce these risks, respondents are focusing most on reducing malware, malicious insiders and server side injections. Such attacks as cross-site scripting and web scraping are less of a priority as shown in Figure 8.

Figure 8: Cyber attacks in terms of a risk mitigation priority
10 = highest to 1 = lowest (converted scale)



This is consistent with what are perceived to be the most significant barriers that are a lack of effective security technology solutions, insufficient visibility of people and business process and lack of skilled or expert personnel as shown in Figure 9.

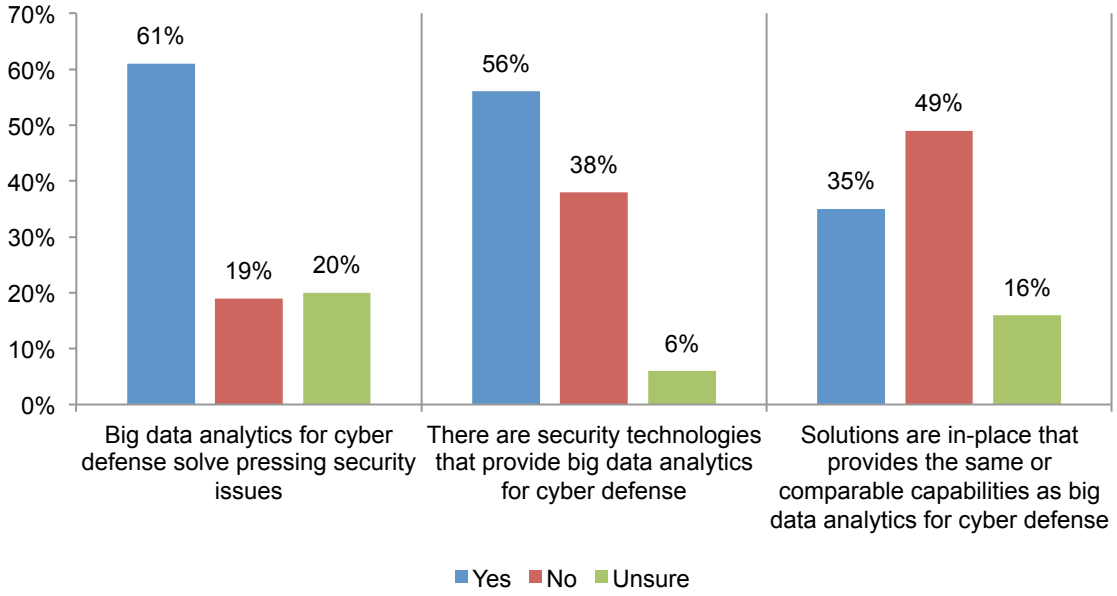
Figure 9: Most significant barriers to achieving a strong cyber security posture
Two responses permitted



Big Data Analytics & Cyber Security Solutions

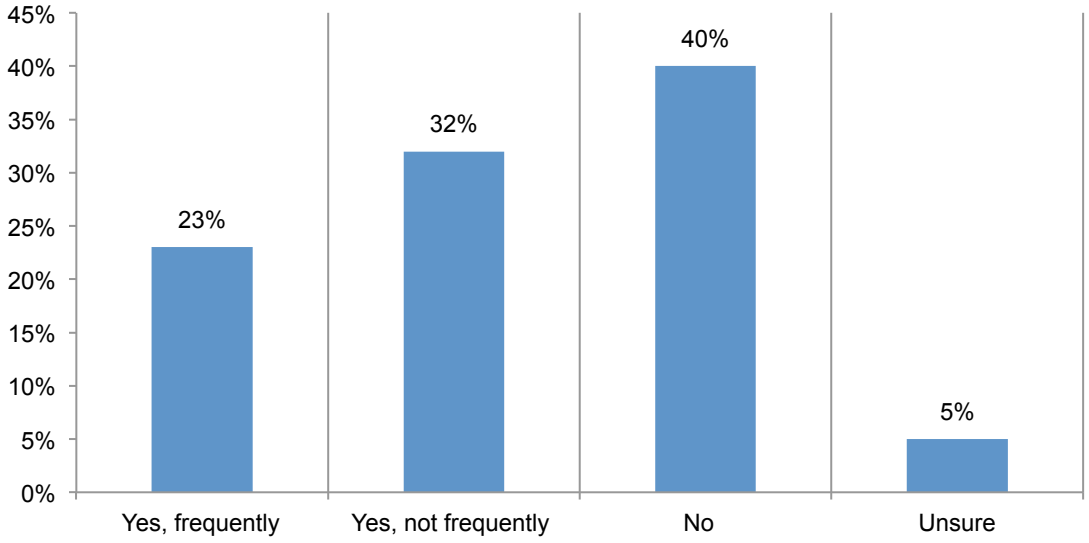
The majority of respondents say they know of security technologies that provide big data analytics for cyber defense and believe they solve pressing security issues faced by their organizations (56 percent and 61 percent, respectively). However, only 35 percent have these solutions in place (Figure 10).

Figure 10: Perceptions about big data analytics



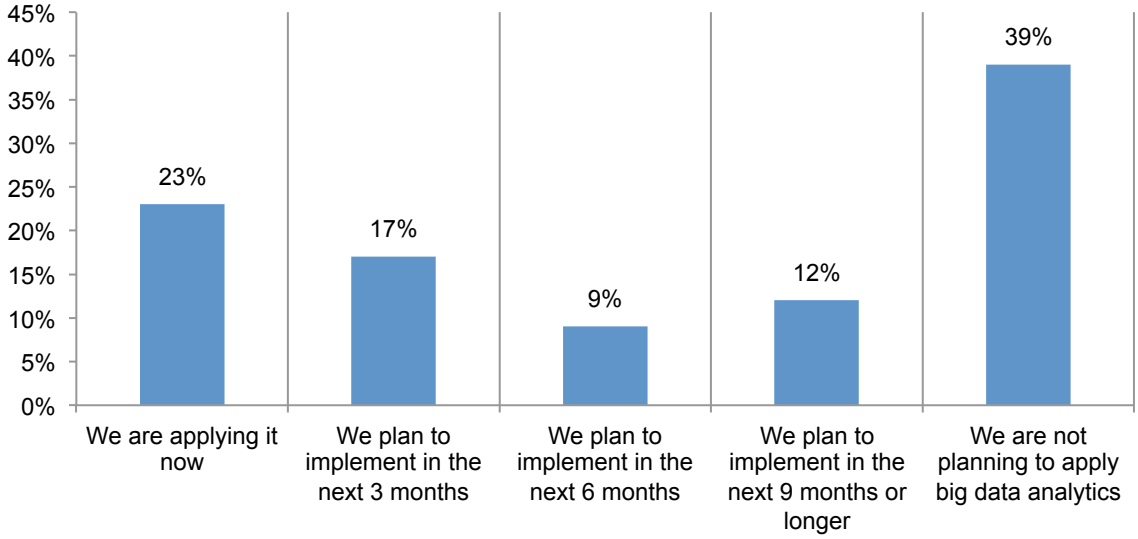
Currently only 23 percent of respondents say their organization frequently uses analytics to determine the origins of attacks and 32 percent say they use analytics infrequently as shown in Figure 11. Reasons for not using analytics (40 percent of respondents) are a lack of enabling intelligence/technologies and lack of ample expert personnel. Other reasons are that they do not determine the origins of attacks (53 percent) or they rely on close examination of logs and configuration settings (41 percent).

Figure 11: Does your organization use analytics to determine the origins of attacks?



According to Figure 12, 61 percent of organizations represented in this study are applying or moving toward the adoption of big data analytics. As discussed later in this report, certain industries are more likely to invest in big data analytics.

Figure 12: Plans to apply big data analytics in cyber defense



Big data analytics and cyber analytics tools allow organizations to recognize patterns of activity that represent network threats. We asked respondents to identify in this context how network data presents both a challenge and opportunity in cyber defense.

As shown in Figure 13, the challenges are data growth, data integration and data complexity. With the exception of data growth, these also present the greatest opportunities to use network data to become more proactive and intelligent about detecting and stopping threats.

Figure 13: The greatest challenges and opportunities with network data
Two choices permitted

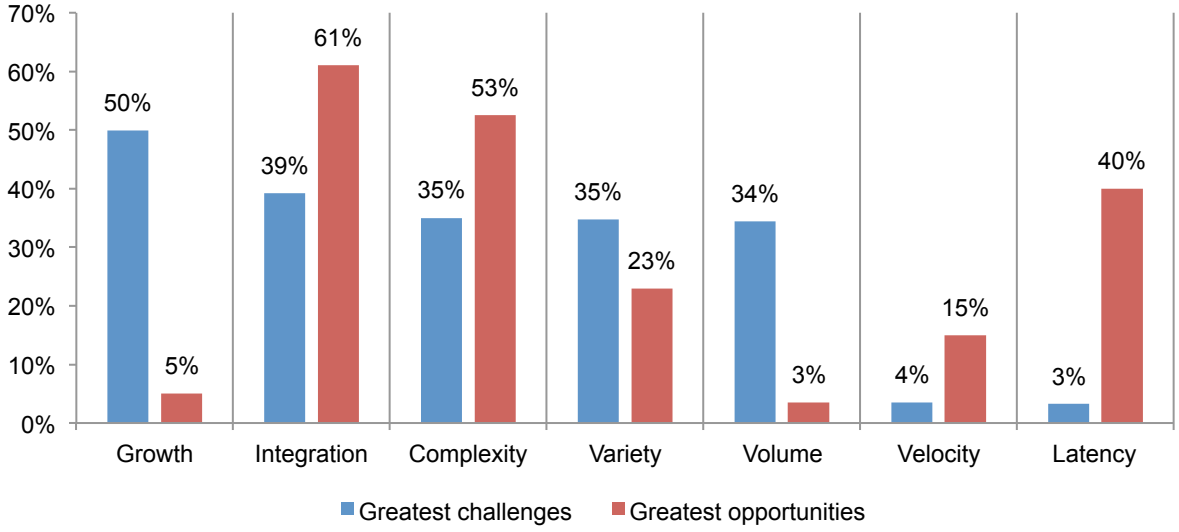
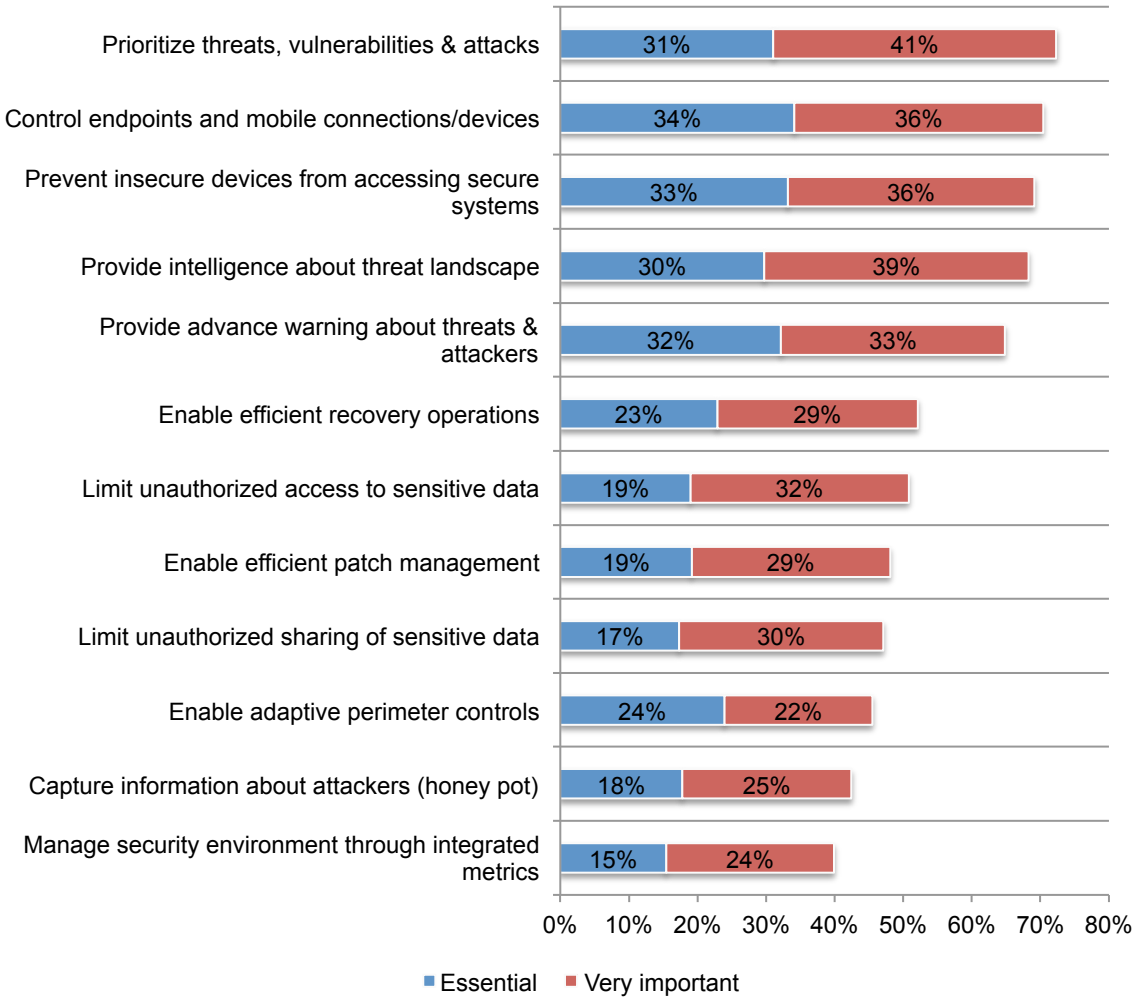


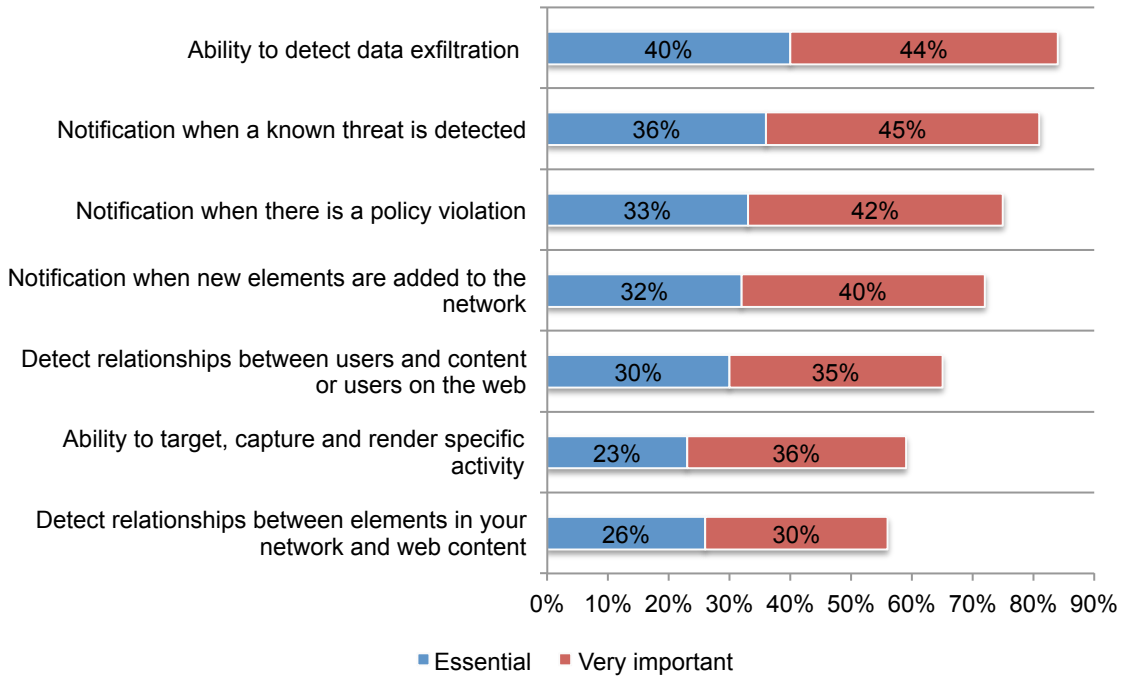
Figure 14 reveals that the most important features for security technologies, according to respondents are: ability to prioritize threats, vulnerabilities and attacks; control of endpoints and mobile connections and devices; prevent insecure devices from accessing secure systems, provide intelligence about threat landscape and provide advance warning about threats and attackers.

Figure 14: The most important features used today for security technologies
Essential and very important response combined



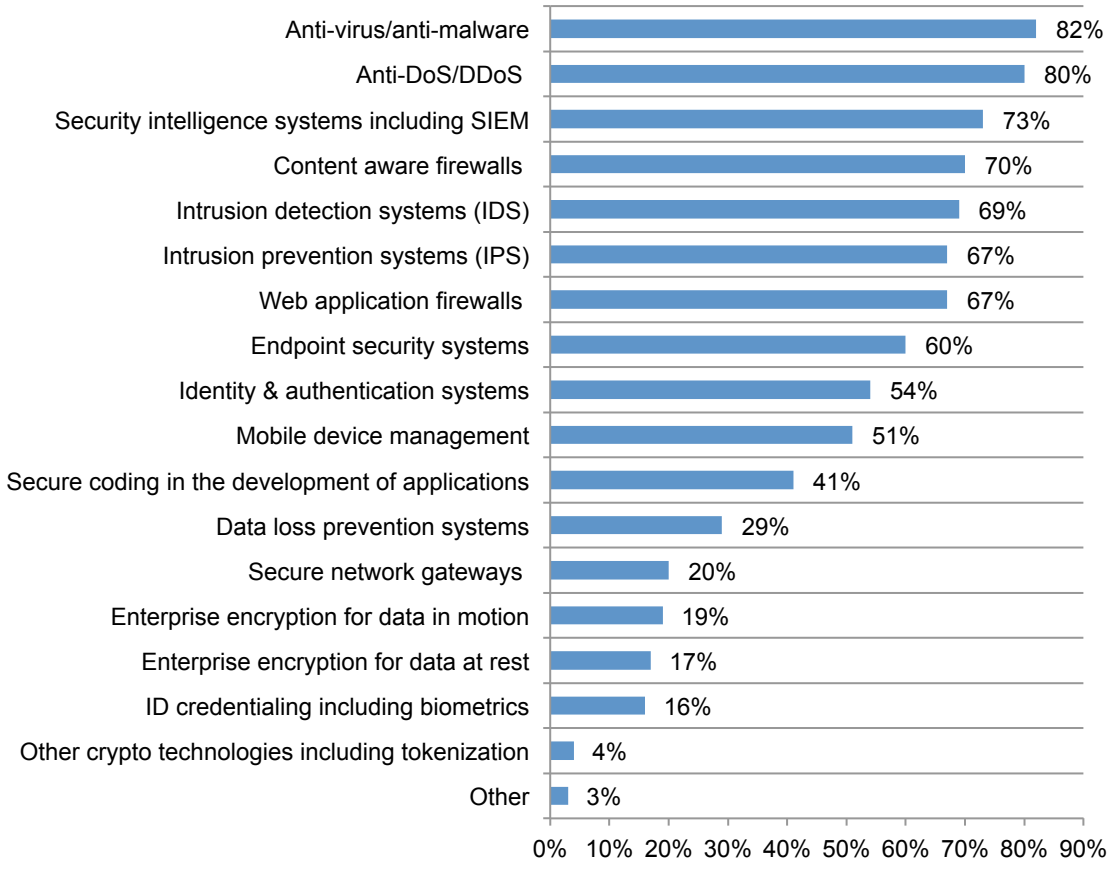
The most important capabilities are: the ability to detect data exfiltration, notification when a known threat is detected (like Botnet), notification when there is a policy violation and notification when new elements are added to the network (Figure 15).

Figure 15: Important capabilities for security technologies
Essential and very important response combined



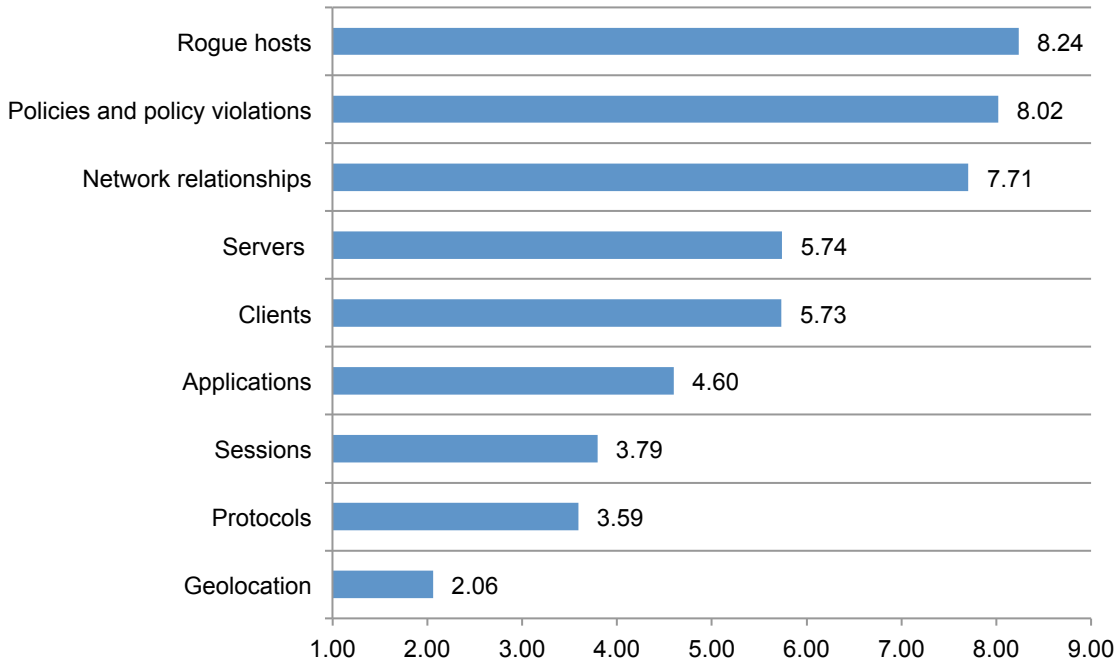
To make their organizations more secure, respondents would most like big data analytics to be combined with anti-virus/anti-malware, anti-DoS/DDoS, security intelligence systems (SIEM) and content aware firewalls as shown in Figure 16. Respondents want to know potential future threats and future data exfiltration.

Figure 16: Enabling technologies combined with big data analytics for better security
More than one response permitted



To securely operate their organization's networks, visibility is most important to understand the activities of rogue hosts, policies and policy violations, network relationships as revealed in Figure 17. Of less importance is visibility to protocols and geolocation.

Figure 17: Where is visibility most important?
9 = most important to 1 = least important (converted scale)



Industry Differences

In this study, we analyzed different perceptions and practices in financial services (FS), manufacturing (Manf) and government (Gov). We present the most salient findings of this analysis in this section.

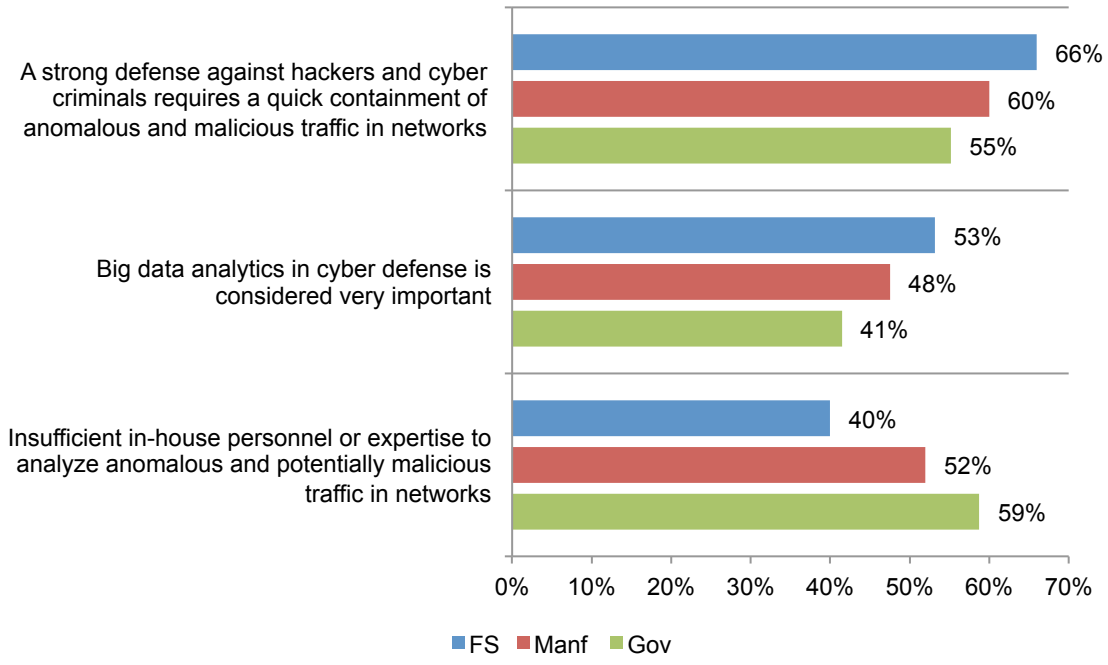
Perceptions about cyber security readiness

Is big data analytics important in cyber defense? There is a significant difference between financial services and government in perception that big data analytics in cyber defense are very important as shown in Figure 18.

Cyber security requires organizations to see and quickly contain anomalous and potentially malicious traffic. A much larger percentage of respondents in financial services agree that launching a strong defense against hackers and other cyber criminals requires their organizations to see and quickly contain anomalous and potentially malicious traffic in their networks (Figure 18).

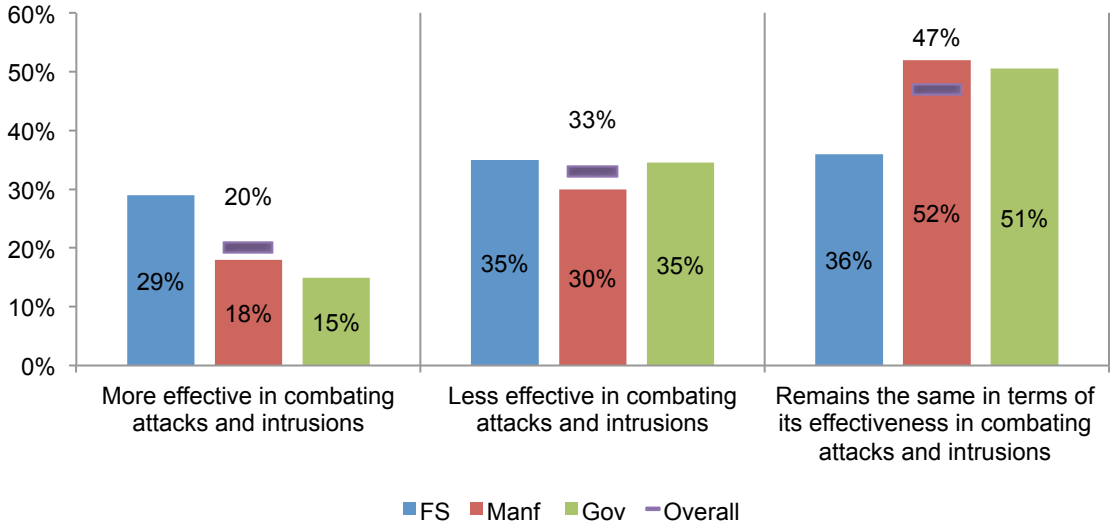
Is the in-house expertise available to analyze anomalous and potentially malicious traffic? Financial services respondents are more likely to agree that they have the in-house personnel or expertise to analyze anomalous and potentially malicious traffic in networks (Figure 18).

Figure 18: Perceptions about prevention & detection of anomalous & malicious traffic
Strongly agree and agree response combined



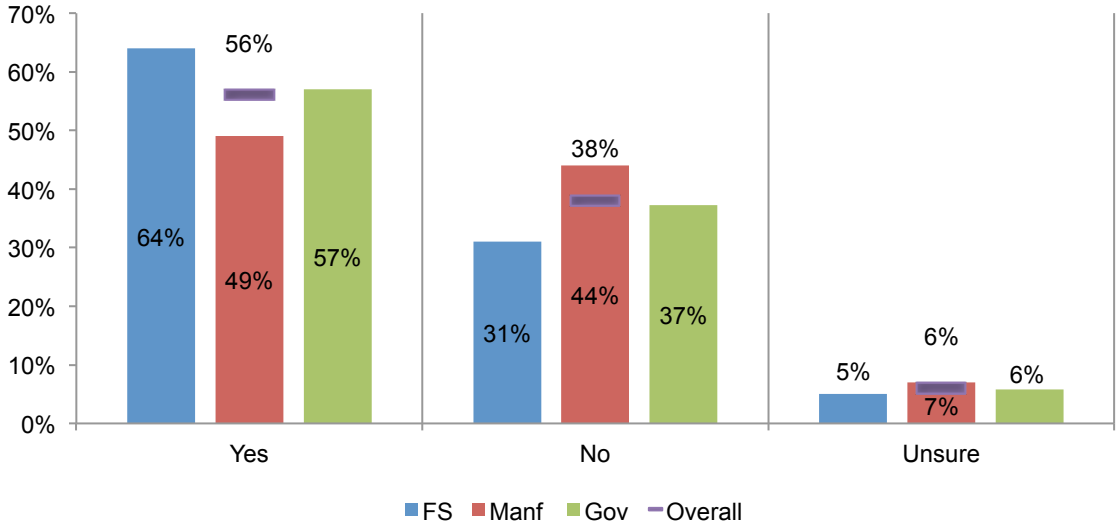
Which industry's cyber effectiveness has increased in the past 12 months? According to Figure 19, respondents in manufacturing are more likely to believe their organizations have stayed the same in the past 12 months. A higher percentage of financial services organizations say their organization's cyber security posture has become more effective.

Figure 19: The cyber security posture over the past 12 months



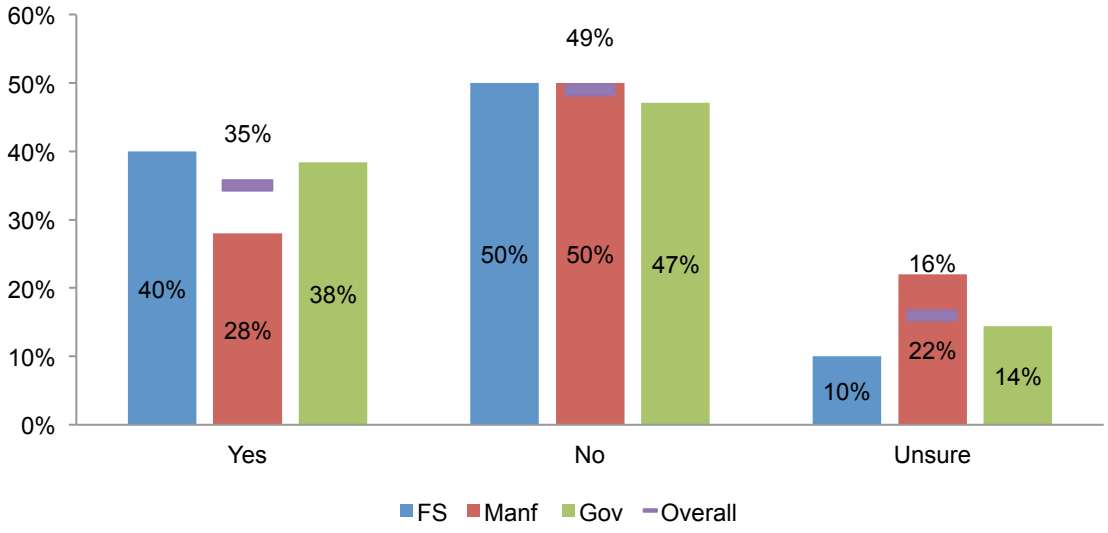
Are industries aware of the availability of big data analytics for cyber defense and do they think they are a solution? Again, the financial services industry is ahead in awareness of big data analytics for cyber defense, as revealed in Figure 20. The majority of respondents in financial services, manufacturing and government believe big data analytics is a solution for dealing with the changing threat landscape (70 percent, 55 percent and 60 percent respectively).

Figure 20: Awareness of security technologies that provide big data analytics



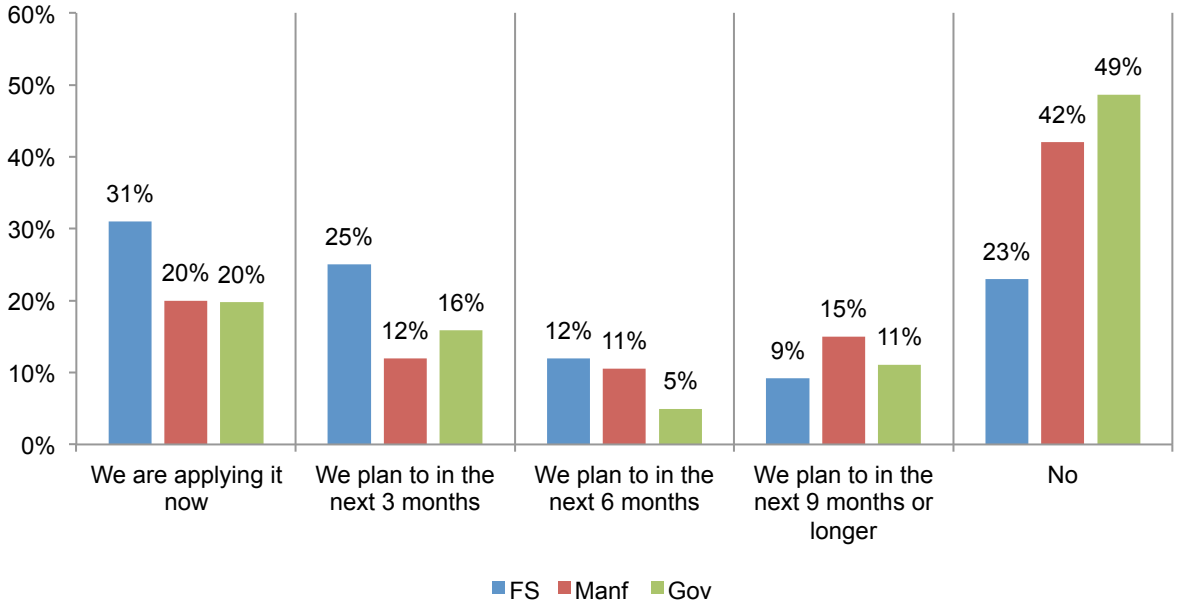
Which industries have solutions that provide the same types of capabilities as big data analytics for cyber defense? While financial services respondents say they have these in place, government is not far behind as shown in Figure 21. Respondents in manufacturing have the greatest uncertainty about the existence of these technologies in their organizations.

Figure 21: Solutions are in-place with comparable capabilities as big data analytics



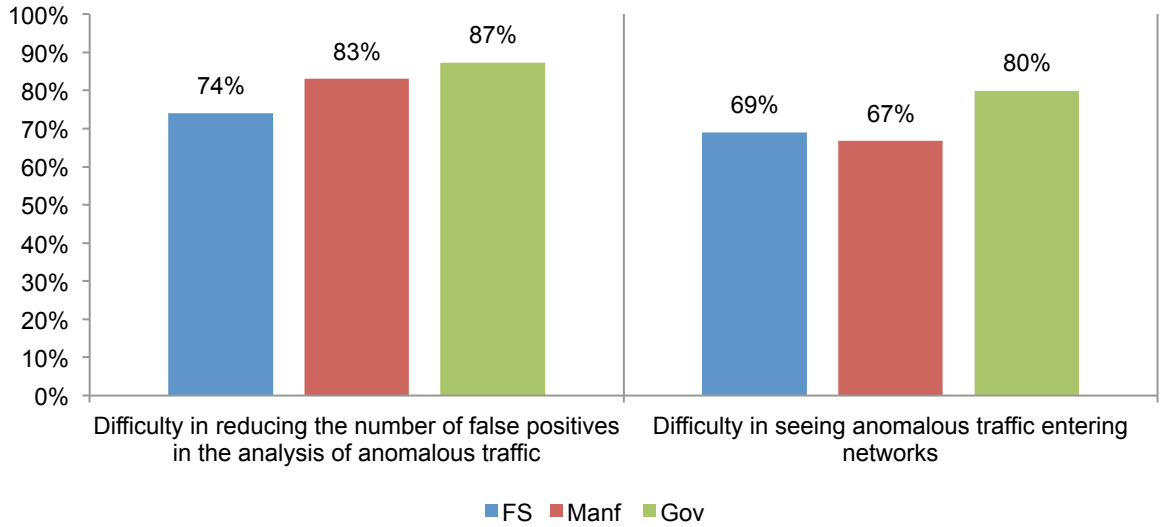
What is the timeline for implementing big data analytics? Based on the findings discussed above, it is no surprise that financial services is moving more aggressively to implement these solutions. In contrast, just about half of the government sector say they do not plan to apply big data analytics in cyber defense as shown in Figure 22.

Figure 22: Plans to apply big data analytics in cyber defense



Respondents in all industries see difficulties in dealing with anomalous traffic. Government and manufacturing see the most difficulty in reducing the number of false positives in the analysis of anomalous traffic as revealed in Figure 23. Financial service is almost evenly divided in difficulty related to stopping anomalous traffic and reducing false positives.

Figure 23: Difficulties with anomalous traffic
Very difficult and difficult response combined



A Message from Teradata

Teradata Corporation commissioned this survey with the Ponemon Institute because we believe that data, when exploited, is an effective weapon in combating cyber security threats. Many of today's organizations have realized that it is no small feat to quickly sift through 99.9% of unimaginable and growing volumes of IP network data to isolate the 0.1% of data which points to anomalous behavior and potential network threats.

Cyber security and network visibility are a big data problem.

Why Teradata? Why is a data warehouse company interested in cyber security?

Those questions have frequently been raised as we look to bring this report to market. For background, Teradata Corporation is a recognized visionary in data warehousing, big data analytics and business applications. Teradata and its partners provide the best technology to industry innovators who embrace the value of data to change processes, business models, performance, and even industries.

How? By transforming all data into information for strategic advantage, and making that information actionable in near-real time through powerful analytic data solutions. For more than 30 years, Teradata's approach to data warehousing has focused on making integrated business data accessible to support enterprise-wide strategic and tactical decisions; while many organizations consider data warehousing to be about storage.

That difference allows Teradata solutions to help more businesses and organizations unlock the enduring value of data. The power of Teradata extends to cyber security where Teradata solutions provide a single, comprehensive, and authoritative environment for integrating and accessing information security and IP network data for faster time to remediation.

Why big data analytics in cyber defense?

The results of the survey confirm that traditional solutions, which continue to fall short in detecting and stopping threats, can be enhanced with big data analytics. Additionally, as borders and boundaries of networks continue to blur with remote connectivity and growing numbers of mobile devices, visibility to network activity becomes more difficult and the potential for weaknesses to be exploited on the network increases.

It's time to move beyond the conventional wisdom which declares that attack volumes and legacy data stores are too large to analyze, the analysis too complex, and processing power too intensive and time consuming to match the pace of cyber attacks. By seeking more responsive solutions, security teams are enabled to become more proactive in their security posture through improved reaction times, more comprehensive forensic investigations and heightened defensive measures.

The survey question that relates directly to the opportunities and challenges characterized by network data points out that data integration is both a top challenge and opportunity; while data growth outweighs all other challenges. New big data tools and data management techniques are emerging that can efficiently handle the volume and complexity of IP network data, and should be part of an enterprise cyber defense strategy that meets complex and large-scale analytic and data management demands.

It's concerning that this survey reveals that while cyber crime is escalating, most organizations are less prepared than they were last year. The survey also reveals that knowledge of existing big data technologies to address this critical issue is low. With the publication of this report we hope that awareness will be raised into existing and emerging technologies that address the risks and dynamics of cyber defense both today and into the future.

We would like to thank the Ponemon Institute for their expertise and guidance in conducting this survey.

For more information about Teradata, please visit http://www.teradata.com/cybersecurity-threat/

Part 3. Methods

A random sampling frame of 18,046 IT or data security practitioners located in all regions of the United States were selected as participants to this survey. As shown in Table 1, 860 respondents completed the survey. Screening removed 96 surveys and an additional 58 surveys that failed reliability checks were removed. The final sample was 706 surveys (or a 3.9 percent response rate).

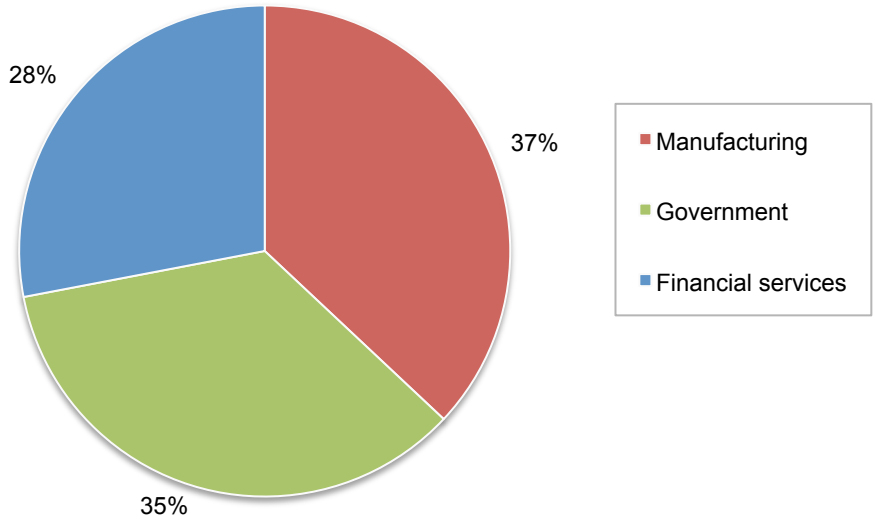
Table 1: Sample response	Freq	Pct%
Total sampling frame	18,046	100.0%
Total returns	860	4.8%
Rejected surveys	58	0.3%
Screened surveys	96	0.5%
Final sample	706	3.9%

As noted in Table 2, the respondents' average (mean) experience in IT, or security experience is 10 years.

Table 2: Other characteristics of respondents	Mean	Median
Total years in IT or security experience	10.06	10.00
Total years in your current position	6.72	7.00

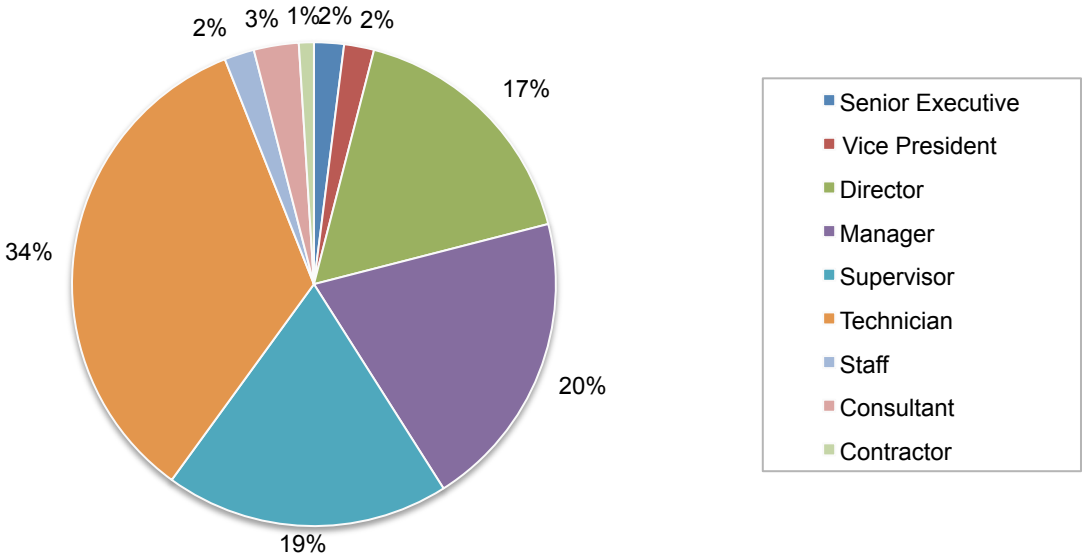
Pie Chart 1 reports the industry segments of respondents' organizations. This chart identifies manufacturing (37 percent) as the largest segment, followed by government (35 percent) and financial services (28 percent).

Pie Chart 1: Industry distribution of respondents' organizations



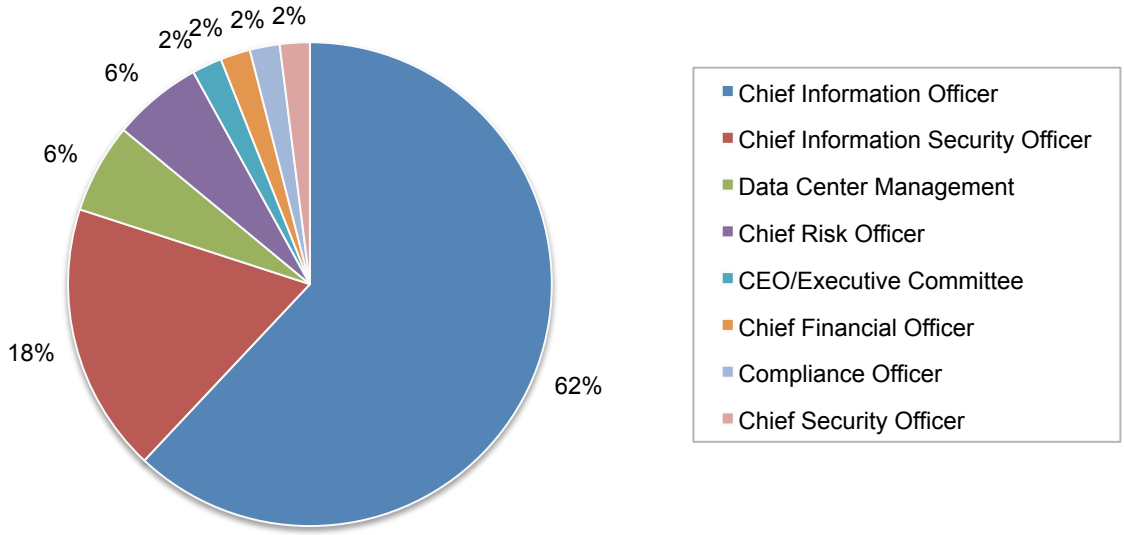
Pie Chart 2 reports the respondent's organizational level within participating organizations. By design, 60 percent of respondents are at or above the supervisory levels.

Pie Chart 2: What organizational level best describes your current position?



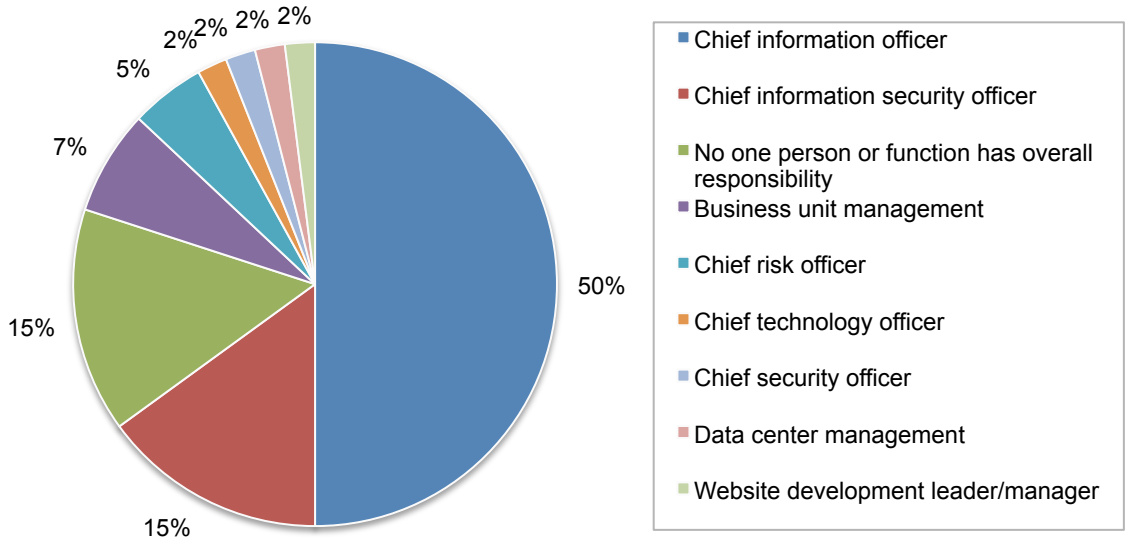
According to Pie Chart 3, 62 percent of respondents report directly to the Chief Information Officer and 18 percent report to the Chief Information Security Officer.

Pie Chart 3: The primary person you or the IT security practitioner reports to within the organization



According to Pie Chart 4, 50 percent of respondents indicated the Chief Information Officer as the person most responsible for managing the organization's cyber security posture.

Pie Chart 4: The primary person most responsible for managing the cyber security posture



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 data security practitioners. 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 holdout 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 a truthful response.

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 December 2012.

Sample response	Freq	Pct%
Total sampling frame	18,046	100.0%
Total returns	860	4.8%
Total rejections	58	0.3%
Screened surveys	96	0.5%
Final sample	706	3.9%

Part 1. Screening questions

S1. How familiar are you with your organization's defense against cyber security attacks?	Freq	Pct%
Very familiar	253	29%
Familiar	372	43%
Somewhat familiar	178	21%
No knowledge	57	7%
Total	860	100%

S2. Do you have responsibility in managing cyber security activities within your organization?	Freq	Pct%
Yes, full responsibility	271	34%
Yes, some responsibility	493	61%
Minimal or no responsibility	39	5%
Total	803	100%

Part 2. Perceptions about the organization

Please rate each statement using the five-point scale provided below the item. Strongly agree and agree response combined.	Strongly agree	Agree
Q1a. My organization considers big data analytics in cyber defense as very important.	21%	26%
Q1b. My organization is vigilant in detecting anomalous and potentially malicious traffic in networks.	21%	28%
Q1c. My organization is vigilant in preventing anomalous and potentially malicious traffic from entering networks.	15%	27%
Q1d. Launching a strong defense against hackers and other cyber criminals requires my organization to see and quickly contain anomalous and potentially malicious traffic in networks.	31%	29%
Q1e. My organization does not have the in-house personnel or expertise to analyze anomalous and potentially malicious traffic in networks.	25%	26%

Part 3. Security environment

Q2. Please rank each one of the following five (5) cyber security threats in terms of threat severity level from 1 = highest severity to 5 = lowest severity.	Average rank	Rank order
Wrongful disclosure	2.23	3
Theft of information assets	1.48	1
Corruption of information	3.74	5
Destruction of property, plant and equipment	3.15	4
Interruption of services	1.92	2

Q3. Please rank each one of the following ten (10) cyber attacks in terms of a risk mitigation priority within your organization from 1 = highest to 10 = lowest priority.	Average rank	Rank order
Malware	1.84	1
Server side injection (SSI)	2.19	3
Cross-site scripting	7.89	9
Denial of service (DoS)	2.60	4
Distributed denial of service (DDoS)	2.96	5
Web scrapping	9.59	10
Viruses, worms and trojans	3.65	7
Botnets	3.39	6
Malicious insiders	2.12	2
Phishing and social engineering	5.34	8

Q4. Please rank each one of the following eight (8) negative consequences that your organization experienced as a result of a cyber attack or intrusion, from 1 = most severe to 8 = least severe.	Average rank	Rank order
Lost intellectual property (including trade secrets)	1.77	1
Stolen or damaged equipment	5.06	6
Productivity decline	2.99	2
Lost revenue	3.74	3
Regulatory actions or lawsuits	6.53	7
Reputation damage	4.33	4
Customer turnover	7.18	8
Cost of outside consultants and experts	4.78	5

Q5. What statement best describes changes to your organization's cyber security posture over the past 12 months?	Pct%
Our organization's cyber security posture is **more effective** in combating attacks and intrusions.	20%
Our organization's cyber security posture is **less effective** in combating attacks and intrusions.	33%
Our organization's cyber security posture remains the same in terms of its effectiveness in combating attacks and intrusions.	47%
Total	100%

Q6. Where are you seeing the greatest areas of potential cyber security risk within your IT environment today? Please select your **top three** choices.	Pct%
Mobile access (either through mobile devices such as smart phones and mobile/remote employees)	44%
Lack of system connectivity / visibility	42%
Multiple global interconnected network systems	40%
Cloud computing infrastructure providers	30%
Insiders (whether malicious or negligent)	29%
Fragmented compliance solutions	26%
Network infrastructure environment (endpoint to gateway)	22%
Virtual computing environments	18%
Desktop or laptop computers	16%
Removable media (USB devices) and /or media (CDs, DVDs)	15%
Across 3rd party applications	9%
Within operating systems	7%
The server environment and data centers	2%
Other (please specify)	1%
Total	300%

Q7. What do you see as the most significant barriers to achieving a strong cyber security posture within your organization today? Please select your **top two** choices.	Pct%
Lack of effective security technology solutions	43%
Insufficient visibility of people and business processes	42%
Lack of skilled or expert personnel	38%
Complexity of compliance and regulatory requirements	27%
Insufficient resources or budget	18%
Insufficient assessment of cyber security risks	15%
Lack of leadership	9%
Lack of oversight or governance	7%
Other (please specify)	1%
Total	200%

Q8. In your opinion, where is your organization's cyber readiness most deficient?	Pct%
Enabling security technologies	36%
Professional and competent staff	35%
Oversight and governance activities	15%
Operational and control activities	13%
Other (please specify)	1%
Total	100%

Q9a. What are your **greatest challenges** with network data? Please select your **top two** choices.	Pct%	Order
Data volume	34%	5
Data velocity	4%	6
Data variety	35%	4
Data growth	50%	1
Data complexity	35%	3
Data integration	39%	2
Data latency	3%	7
Total	200%	

Q9b. What are your **greatest opportunities** with network data? Please select your **top two** choices.	Pct%	Order
Data volume	3%	7
Data velocity	15%	5
Data variety	23%	4
Data growth	5%	6
Data complexity	53%	2
Data integration	61%	1
Data latency	40%	3
Total	200%	

Part 4. Security tools & technologies

Q10. What are the most important features for security technologies used in your organization? Please rate each feature using the following scale: 1=essential, 2 = very important, 3 = important, 4 = not important.	Essential	Very important
Prioritize threats, vulnerabilities and attacks	31%	41%
Control endpoints and mobile connections/devices	34%	36%
Prevent insecure devices from accessing secure systems	33%	36%
Provide intelligence about threat landscape	30%	39%
Provide advance warning about threats and attackers	32%	33%
Enable efficient recovery operations.	23%	29%
Limit unauthorized access to sensitive or confidential data	19%	32%
Enable efficient patch management	19%	29%
Limit unauthorized sharing of sensitive or confidential data	17%	30%
Enable adaptive perimeter controls	24%	22%
Capture information about attackers (honey pot)	18%	25%
Manage security environment through integrated metrics	15%	24%

Q11a. Are you aware of any security technologies or solutions that provide big data analytics for cyber defense (as noted above)?	Pct%
Yes	56%
No	38%
Unsure	6%
Total	100%

Q11b. Does big data analytics for cyber defense, as defined above, solve pressing security issues faced by your organization today?	Pct%
Yes	61%
No	19%
Unsure	20%
Total	100%

Q11c. Does your organization have solutions in-place today that provides the same or comparable capabilities as big data analytics for cyber defense (as noted above)?	Pct%
Yes	35%
No	49%
Unsure	16%
Total	100%

Q12. Which of the following cyber defenses employed by your organization, when enhanced with big data analytics for cyber defense, would make your existing environment more secure? Please check all that apply.	Pct%
Anti-virus/anti-malware	82%
Anti-DoS/DDoS (denial of services & distributed denial of services)	80%
Security intelligence systems including SIEM	73%
Content aware firewalls including next generation firewalls (NGFW)	70%
Intrusion detection systems (IDS)	69%
Web application firewalls (WAF)	67%
Intrusion prevention systems (IPS)	67%
Endpoint security systems	60%
Identity and authentication systems	54%
Mobile device management	51%
Secure coding in the development of new applications	41%
Data loss prevention systems	29%
Secure network gateways including virtual private networks (VPN)	20%
Enterprise encryption for data in motion	19%
Enterprise encryption for data at rest	17%
ID credentialing including biometrics	16%
Other crypto technologies including tokenization	4%
Other (please specify)	3%

Q13. Where is visibility most important to securely operating your organization's networks? Please rank the following nine items from 1 = most important to 9 = least important.	Average rank	Rank order
Servers	4.26	4
Clients	4.27	5
Network relationships	2.29	3
Applications	5.40	6
Policies and policy violations	1.98	2
Protocols	6.41	8
Sessions	6.21	7
Geolocation	7.94	9
Rogue hosts	1.77	1

Q14. How important is it to be able to have the following capabilities (1= essential, 2 = very important, 3= important, 4= somewhat important, 5= not important)	Essential	Very important
Ability to detect data exfiltration	40%	44%
Notification when a known threat is detected (like Botnet)	36%	45%
Notification when there is a policy violation	33%	42%
Notification when new elements are added to the network	32%	40%
Detect relationships between users and content or users on the web	30%	35%
Ability to target, capture and render specific activity	23%	36%
Detect relationships between elements in your network and web content	26%	30%

Q15. What types of issues do you want to identify **before** they occur? Please select only your top two choices.	Pct%
Potential future threats	70%
Potential future data exfiltration	64%
Potential network bottlenecks	42%
Potential traffic growth	12%
Potential future user growth	12%
Other (please specify)	0%
Total	200%

Q16a. Does your organization use analytics to determine the origins of attacks?	Pct%
Yes, frequently	23%
Yes, not frequently	32%
No	40%
Unsure	5%
Total	100%

Q16b. If you said no, what are the main reasons why your organization does not use analytics to determine the origins of attacks? Please select only your top two reasons.	Pct%
Lack of enabling intelligence/technologies	67%
Do not have ample expert personnel	65%
Lack of resources or budget	41%
Not considered a security-related priority	27%
Other (please specify)	0%
Total	200%

Q16c. If you said no, how does your organization determine the origins of attacks? Please select all that apply.	Pct%
We do not determine the origins of attacks	53%
Close examination of logs and configuration settings	41%
Use of security intelligence/technologies	24%
Manual surveillance methods	23%
Automated capabilities	5%
Other (please specify)	0%
Total	146%

Q17. Does your organization plan to apply big data analytics in cyber defense?	Pct%
Yes, we are applying it now	23%
Yes, we plan to implement a project in the next 3 months	17%
Yes, we plan to implement a project in the next 6 months	9%
Yes, we plan to implement a project in the next 9 months or longer	12%
No, we are not planning to apply big data analytics in cyber defense	39%
Total	100%

Very difficult and difficult responses combined.	Very difficult	Difficult
Q18a. Please rate the level of difficulty in seeing anomalous traffic entering your organization's networks.	43%	29%
Q18b. Please rate the level of difficulty in stopping anomalous traffic.	47%	30%
Q18c. Please rate the difficulty in reducing the number of false positives in the analysis of anomalous traffic.	49%	33%

Q19, Where does the IT security budget reside in your organization?	Pct%
IT department	54%
Information security department	21%
Security (including facilities management)	4%
Shared among various departments	19%
Other (please specify)	2%
Total	100%

Part 5. Your role and organization

D1. What organizational level best describes your current position?	Pct%
Senior Executive	2%
Vice President	2%
Director	17%
Manager	20%
Supervisor	19%
Technician	34%
Staff	2%
Consultant	3%
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	2%
Chief Financial Officer	2%
General Counsel	0%
Chief Information Officer	62%
Chief Information Security Officer	18%
Compliance Officer	2%
Human Resources VP	0%
Chief Security Officer	2%
Data Center Management	6%
Chief Risk Officer	6%
Other	0%
Total	100%

Experience	Mean	Median
D3a. Total years of IT or security experience	10.06	10.00
D3b. Total years in current position years	6.72	7.00

D4. Who is **most responsible** for managing your organization's cyber security posture?	Pct%
Chief information officer (CIO)	50%
Chief technology officer (CTO)	2%
Chief information security officer (CISO)	15%
Chief security officer (CSO)	2%
Chief risk officer (CRO)	5%
Data center management	2%
Business unit management	7%
Website development leader/manager	2%
Corporate compliance or legal department	0%
Outside managed service provider (MSSP)	0%
No one person or function has overall responsibility	15%
Other	0%
Total	100%

D5. What industry best describes your organization's industry focus?	Pct%	Sub-totals
Financial services		28%
Banking	14%	
Investment management	3%	
Brokerage	4%	
Insurance	2%	
Credit cards and payments	4%	
Other	1%	
Manufacturing		37%
Aerospace	3%	
Automotive	3%	
Industrial equipment	2%	
Energy	5%	
Chemicals	2%	
Consumer products	7%	
Pharmaceuticals	4%	
High tech	9%	
Other	2%	
Government		35%
Federal: defense	9%	
Federal: civilian	8%	
Federal: intelligence	5%	
State government	6%	
Local/municipal government	5%	
Other	2%	
Total	100%	100%

D6. Where are your employees located? (Check all that apply):	Pct%
United States	100%
Canada	69%
Europe	70%
Asia-Pacific	58%
Middle East & Africa	41%
Latin America	50%

D7. What is the worldwide headcount of your organization?	Pct%
Less than 1,000	7%
1,001 to 5,000	41%
5,001 to 25,000	28%
25,001 to 75,000	16%
More than 75,000	8%
Total	100%
Extrapolated global headcount	19,899

D8. What is your organization's annual revenue (US dollars)?	Pct%
Less than $500 million	6%
$501 million to $1 billion	21%
$1 billon to $10 billion	45%
More than $10 billion	28%
Total	100%
Extrapolated total annual revenues ($millions)	$5,742

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.

EB-7499 02.13