Ponemon INSTITUTE

Efficacy of Emerging Network Security Technologies

Sponsored by Juniper Networks

Independently conducted by Ponemon Institute LLC

Publication Date: February 2013

Efficacy of Emerging Network Security Technologies

Ponemon Institute, February 2013

Part 1. Introduction

The purpose of the *Efficacy of Emerging Network Security Technologies* study sponsored by Juniper Networks and conducted by Ponemon Institute is to learn about organizations' use and perceptions about emerging network security technologies and their ability to address serious security threats. The emerging technologies examined in this study include next generation firewalls, intrusion prevention systems with reputation feeds and web application firewalls.

In this study, we surveyed 4,774 IT and IT security practitioners in the following nine countries: United States, United Kingdom, Australia, Germany, France, India, Japan, China and Brazil. All respondents are familiar with their organization's emerging network security technologies and deployment strategy. On average they have approximately 10 years IT or IT security experience.

According to the participants in this research, the reasons for investing in emerging network security technologies are the growing sophistication of cyber attacks and changing threat landscape. Prevention of security breaches and frequency of cyber attacks are not the most important drivers for investing in these technologies.

The issues that keep most IT and IT security practitioners up at night are the theft of their organization's intellectual property, including research and development, business strategies and industrial processes. Another target of network attackers is confidential information used to obtain authentication credentials to infiltrate networks and enterprise systems.

Following are some noteworthy takeaways based on the consolidated findings:

- Securing web traffic is by far the most significant network security concern for the majority of organizations. However, the majority of respondents say network security technologies fall short of vendors' promises.
- Almost half (48 percent) of respondents agree that emerging network security technologies are not effective in minimizing attacks that aim to bring down web applications or curtail gratuitous Internet traffic.
- Emerging network security technologies only address part of the cyber security attacks perpetrated upon their organizations. Evidence of this limitation is the finding that most organizations in this study report an average of two successful security breaches in the past two years.
- Companies remain focused on the inside-out threat.[1] However, the rise of external attacks suggests security technology investments need to be more comprehensive and holistic.
- NGFWs and WAFs are often deployed in monitor only and non-blocking modes because of concerns about false positives. This concern appears to affect a majority of the installed base. This suggests that as a threat mitigation regimen the combination of emerging technologies is not as effective as one would hope in stemming the exfiltration of confidential information and network breach.
- Emerging network security technologies work best in reducing general malware, rootkits and advanced malware. Not as effective is their ability to deal with zero day attacks, hacktivism and SQL injections.

[1] The inside-out threat is about devices that sit inside the network that become infected and consequently used as a vector for data exfiltration. This is less about unwitting or malicious insiders and more about nefarious inside traffic resulting from the use of risky apps that lead to device infection and data loss.

Part 2. Key Findings

We organized this research according to the following topics:

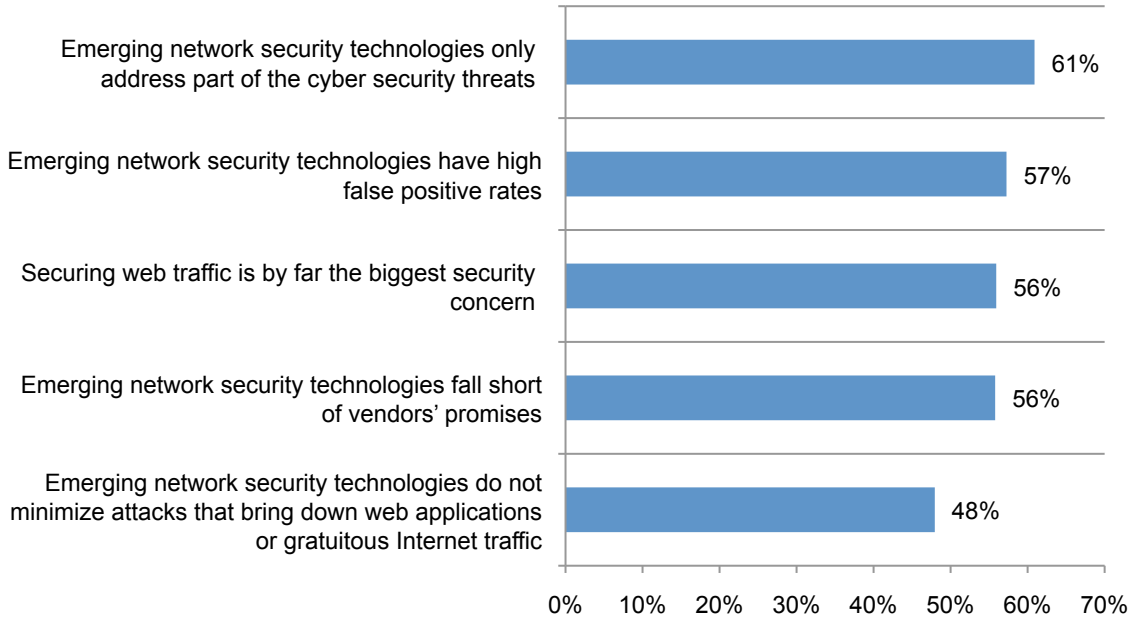
- Perceptions about emerging network technologies
- Network security posture of participating organizations
- Efficacy in addressing network security risks

Perceptions about emerging network technologies

Do emerging network security technologies meet expectations? The majority of respondents (56 percent) say securing web traffic is their biggest security concern, as shown in Figure 1. However, an even larger percentage of respondents, (61 percent) say emerging network security technologies only address part of the cyber security threats facing their organization.

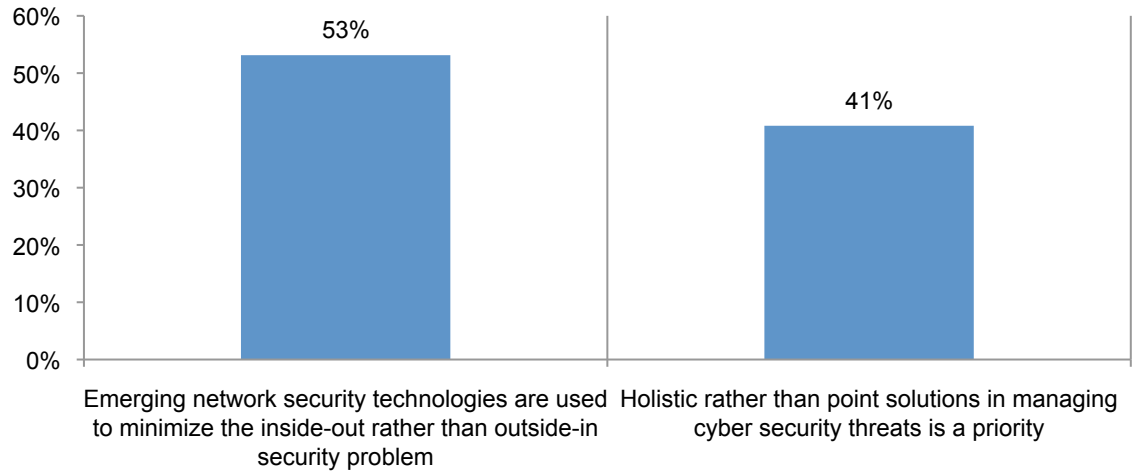
Other issues include the problem of emerging network security technologies having high false positive rates (57 percent of respondents) and 56 percent say emerging network security technologies fall short of vendors' promises. Almost half (48 percent) of respondents agree that emerging network security technologies are not as effective as they should be and do not minimize attacks that bring down web applications or gratuitous Internet traffic.

Figure 1: Attributions about emerging network security technologies
Strongly agree and agree response combined



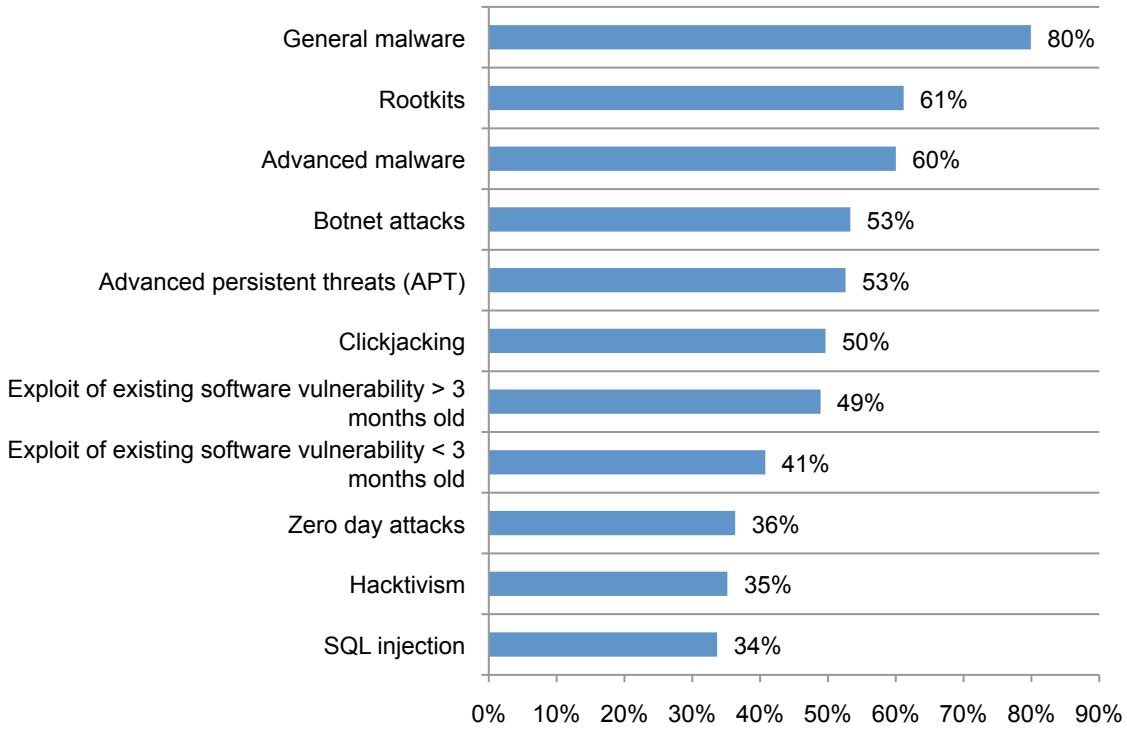
Organizations focus on the inside-out threat and, hence, do not take a more holistic approach to managing cyber security risks. When asked respondents their level of agreement with the statement, "My organization primarily uses emerging network security technologies to minimize the inside-out rather than the outside-in network security problem," 53 percent of respondents agree that their organization primarily uses emerging network security technologies to minimize the inside-out problem (Figure 2). Further, their approach is often to prioritize the point solution in managing cyber security threats. Only 41 percent say the holistic approach would be prioritized.

Figure 2: Perceptions about the management of cyber attacks
Strongly agree and agree response combined



Where emerging network security technologies work best. Figure 3 shows where respondents believe emerging network security technologies are most effective. These are minimizing general malware, rootkits and advanced malware. What is considered less effective is to minimize hacktivism and SQL injections.

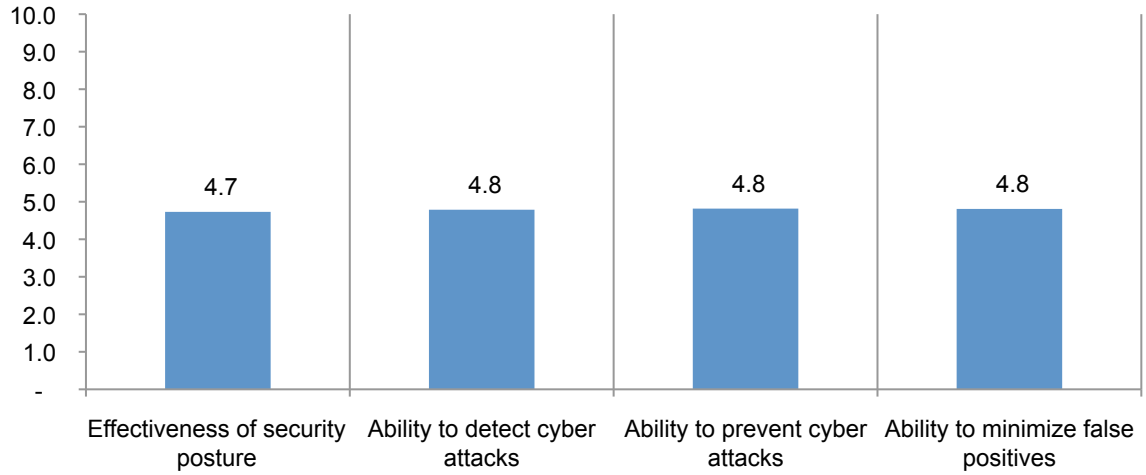
Figure 3: Effectiveness of emerging network security technologies
Very effective and effective response combined



Network security posture of organizations in this study

Figure 4 is a report card on how respondents grade their organizations approach to dealing with network security threats. On average, respondents say the security posture of their organization is only 4.7 based on a scale of 10 being very effective. It seems that this rating may be another indication why organizations on average experienced two data breaches in the past 12 months.

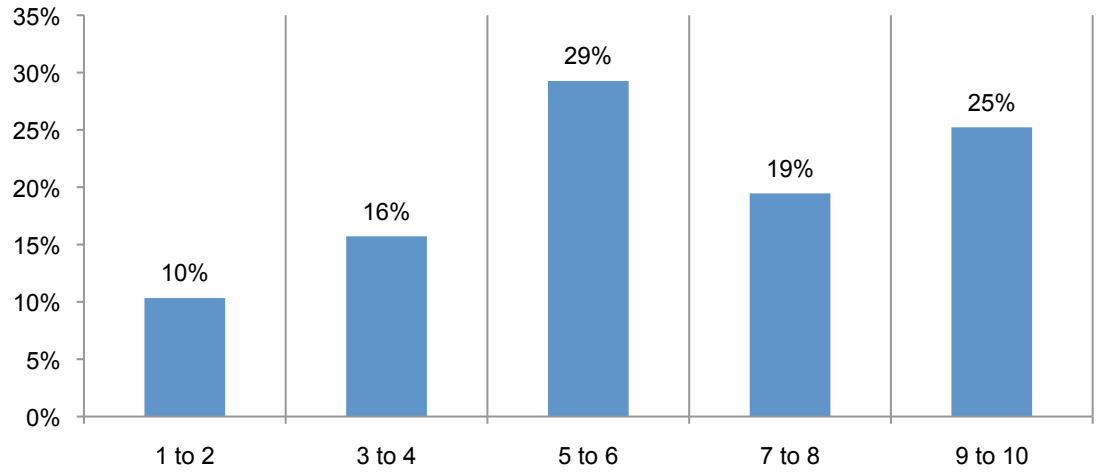
Figure 4: Network security posture
Not effective =1 to very effective = 10
(Extrapolated average reported)



Respondents also rate their organization's ability to quickly detect cyber attacks and prevent cyber attacks as poor (4.8 on a scale of 10 being most effective). Also, their ability to minimize false positives in identifying and containing cyber attacks against networks is not very effective.

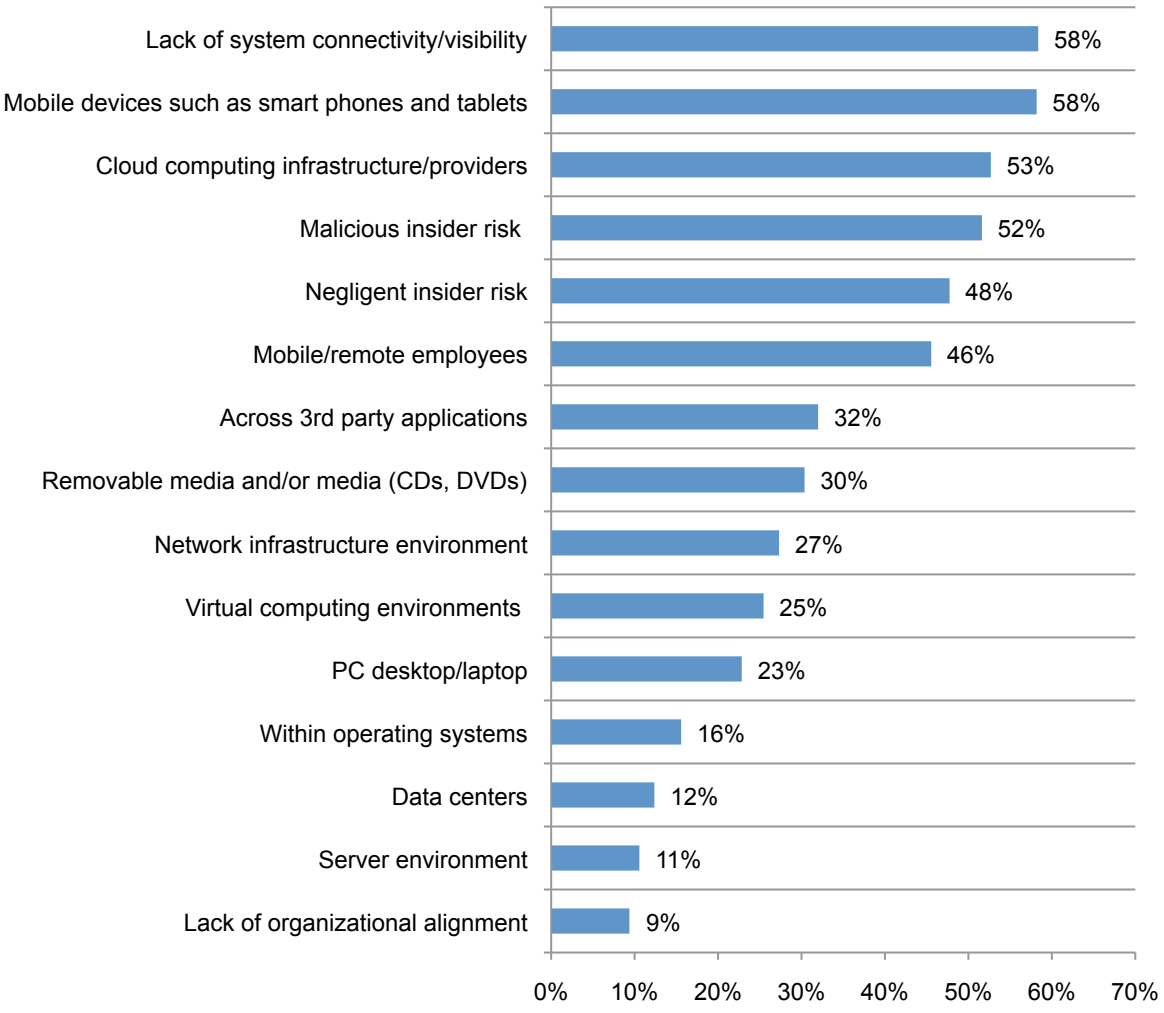
However, as shown in Figure 5, respondents are much more positive about their organization's IT security personnel in terms of their knowledge and expertise in managing emerging network security technologies (6.2 on a scale of 10 being the highest). This could be due to the finding that less than half (49 percent) of respondents say emerging network security technologies used by their organization are dependent upon in-house personnel who possess the knowledge and expertise to operate them effectively.

Figure 5: Level of IT security personnel knowledge and expertise
Very low =1 to very high = 10 (Extrapolated value 6.2)



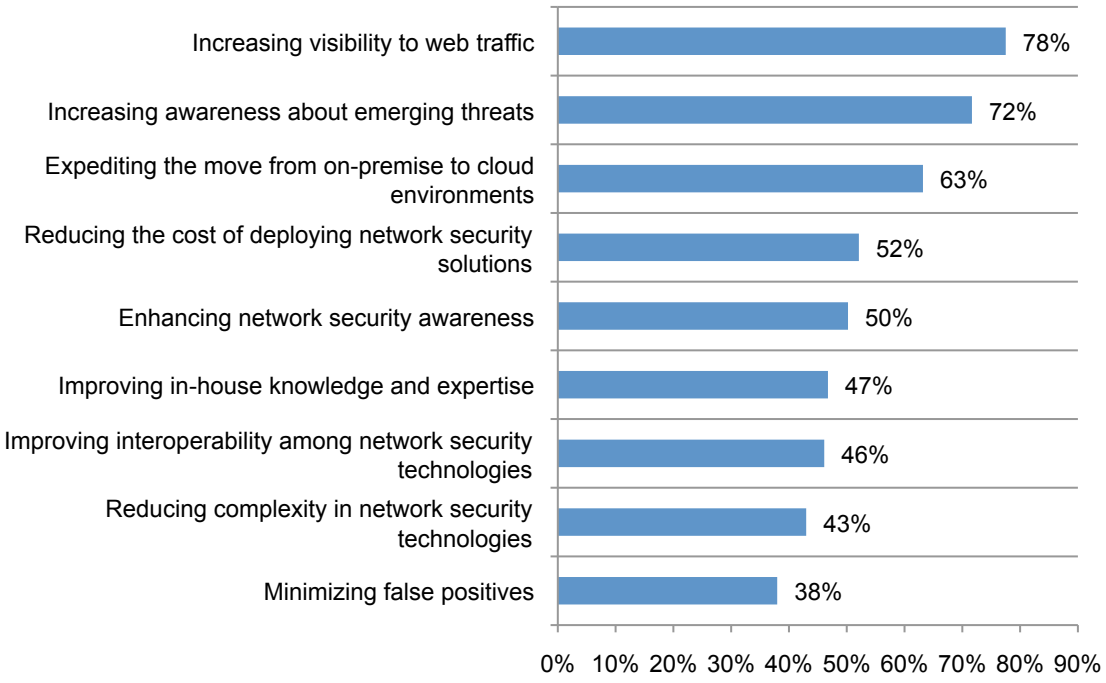
What are perceived as the greatest risks to network security and threaten their network security posture? These are a lack of system connectivity/visibility, mobile devices (such as smart phones and tablets), cloud computing infrastructure/providers and malicious insider risk, according to Figure 6. Considered to be posing the least risk are the network server environment, data centers and lack of organizational alignment.

Figure 6: Greatest rise of potential network security risk
Five choices permitted



What are the network security priorities for organizations? Figure 7 reveals that respondents believe their organizations should increase visibility to web traffic, raise awareness about emerging threats and expedite the move from on-premise to cloud environments. Of less a priority is minimizing false positives and reducing complexity in network security technologies.

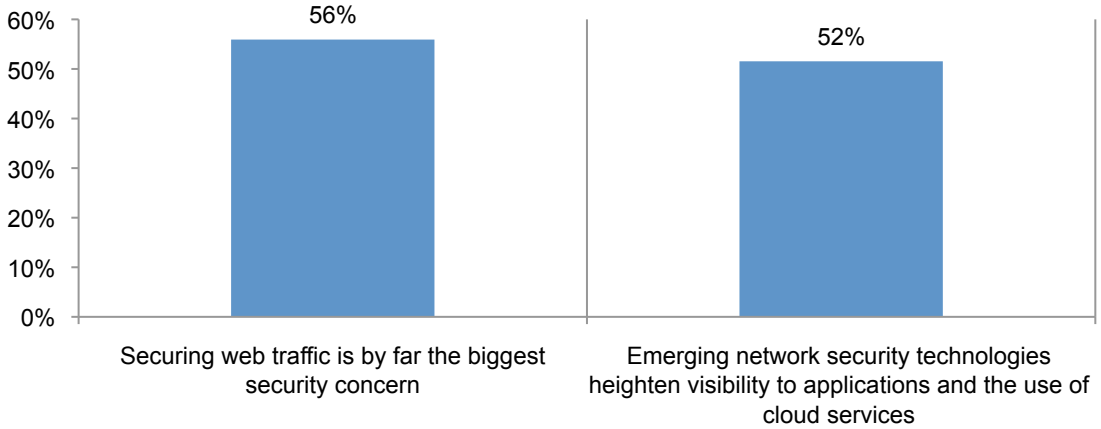
Figure 7: Network security priorities
High priority response



Efficacy of emerging network security technologies

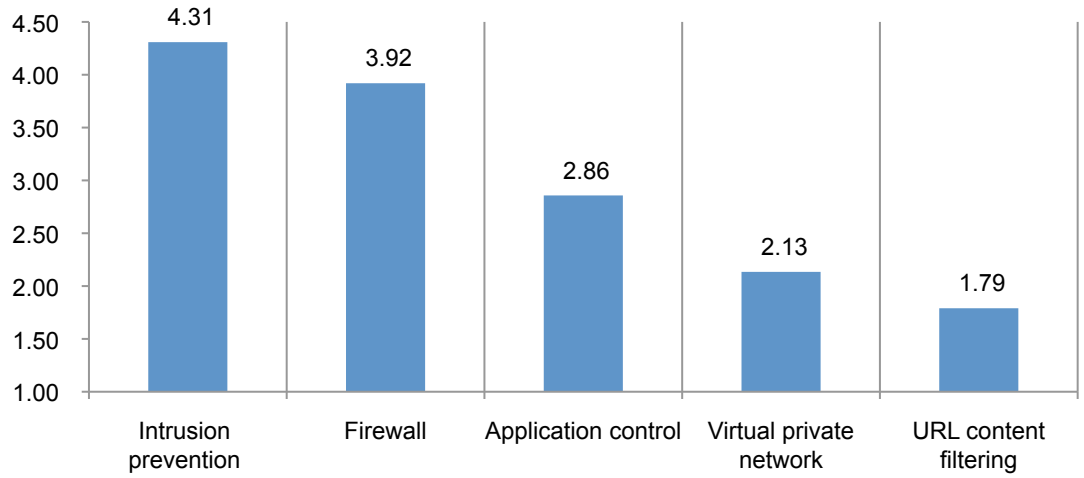
Securing web traffic and increasing visibility to applications and the cloud are important. The majority of respondents (56 percent) say that securing web traffic is by far the biggest network security concern for their organizations, according to Figure 8. More than half (52 percent) of respondents say their organizations use emerging network security technologies to heighten visibility to applications and the use of cloud services.

Figure 8: Attributions about emerging network security technologies
Strongly agree and agree response combined



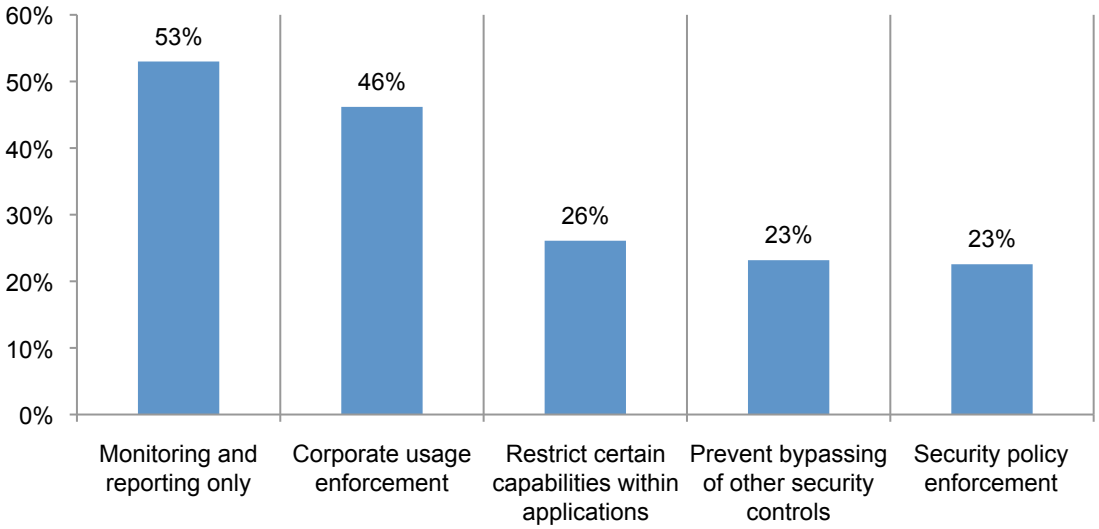
NGFW offers pluses and minuses. More than half (53 percent) of respondents say their organization's NGFW suffers performance degradation when deploying the IPS feature and 21 percent are unsure. Intrusion prevention systems (IPS) and firewalls are the most effective features in the NGFW in the control of the security of the organization's network, according to Figure 9.

Figure 9: Most effective in security
5 = most effective to 1 = least effective (converted scale)



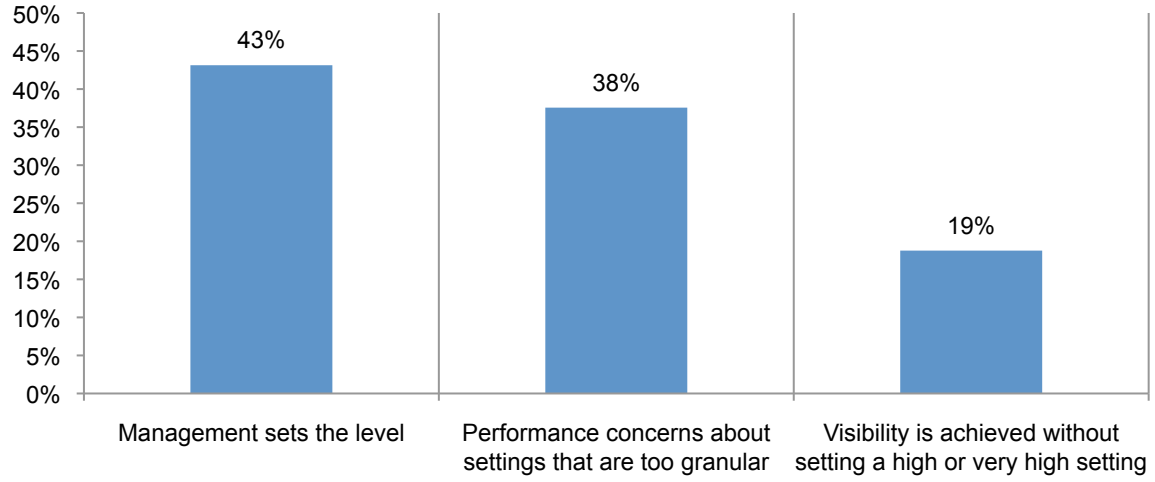
As shown in Figure 10, the application control feature in NGFW is most often configured for monitoring and reporting only (53 percent of respondents).

Figure 10: Configuration of next generation firewalls (NGFW)
More than one response permitted



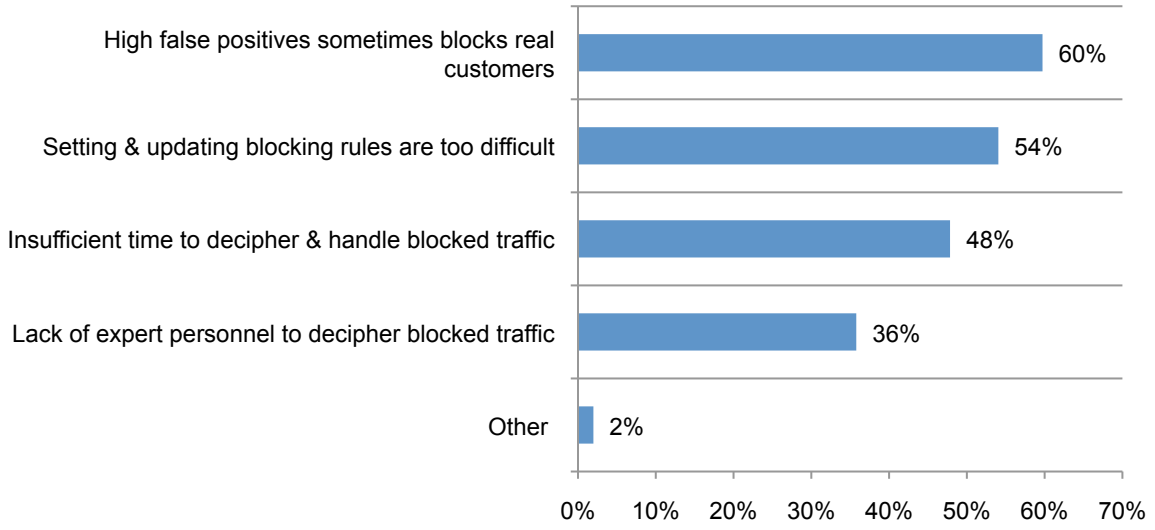
The reasons for not having granularly configured application controls are shown in Figure 11. For many organizations it is that management sets the level and there are performance concerns about settings that are too granular.

Figure 11: Reasons for not having granularly configured application control



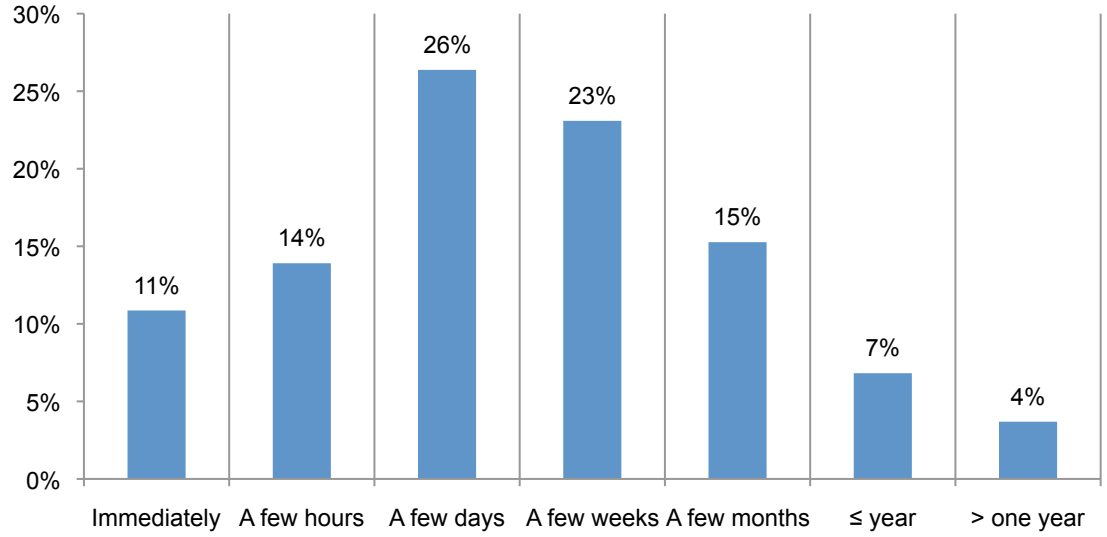
Concerns about false positives curtail use of WAF. Forty-two percent of respondents say their organization deploys WAF in block mode. Figure 12 shows the reasons 58 percent of respondents do not deploy or are unsure. The biggest concern is that its use will affect revenues. Sixty percent of respondents say if they don't use WAF it is because of the high false positives that sometimes block real customers. This is followed by the difficulty in setting and updating blocking rules or policies.

Figure 12: Reasons why WAF is not deployed in block mode
More than one response permitted



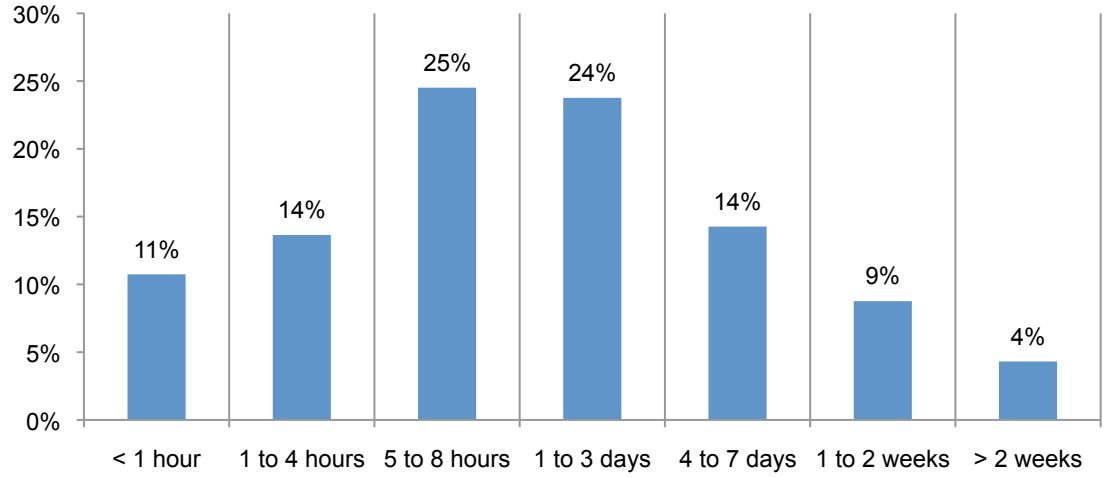
A significant amount of time is spent setting up, configuring and updating rules or policies for WAF. Only 25 (11 + 14) percent of respondents say they can immediately to within a few hours set up and configure their organization's WAF. As shown in Figure 13, the majority of respondents say that it can take at least a few weeks to accomplish these tasks.

Figure 13: Length of time to set up and configure WAF



Similarly, the following chart reveals that technicians can spend several days each month to update rules or policies for each WAF. It also can take days each month to update rules or policies for each WAF, as shown in Figure 14.

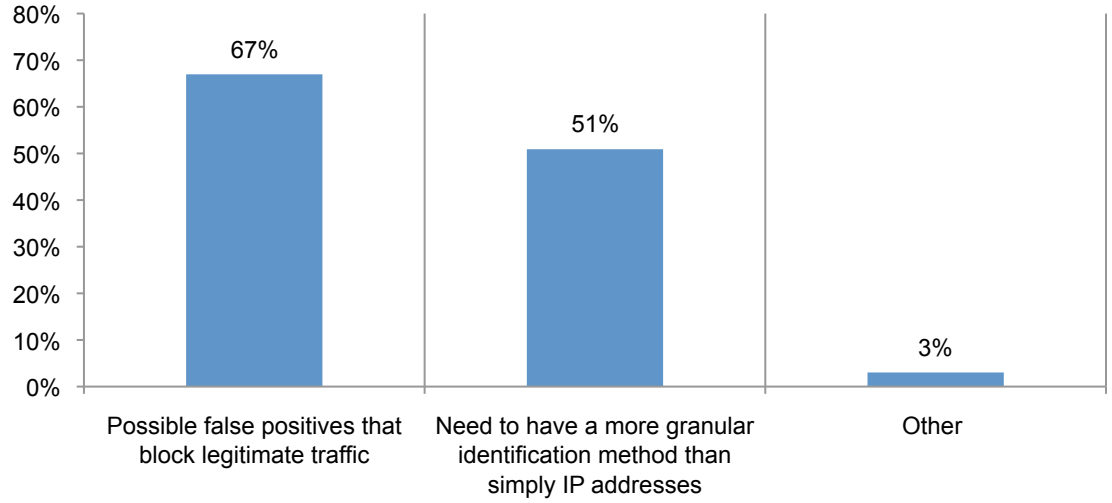
Figure 14: IT/tech time spent each month updating rules or policies for each WAF



Respondents are almost evenly divided about whether the blocking of IP addresses is an effective security measure. Forty-seven percent of respondents believe it is effective, 44 percent say it is not effective and 8 percent are unsure.

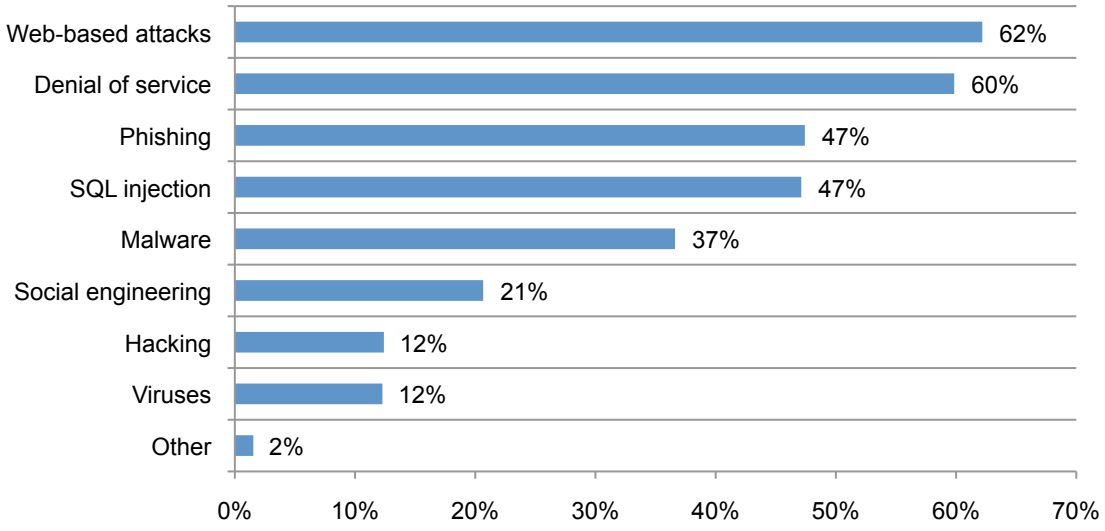
Does the blocking of IP addresses make respondents uncomfortable? Forty-seven percent say they are uncomfortable, however 42 say it doesn't bother them and 11 percent are unsure. As shown in Figure 15, those respondents who say they are uncomfortable do so because possible false positives could block legitimate traffic and the desire for a more granular identification method than simply IP addresses.

Figure 15: Reasons for feeling uncomfortable blocking IP addresses
More than one response permitted



By far the two most serious types of cyber attacks are web-based attacks and denial of service attacks as shown in Figure 16. Least are viruses and hacking. On average respondents say their organization's network security has been successfully breached about two times in the past 12 months.

Figure 16: The most serious types of cyber attacks experienced
Three choices permitted



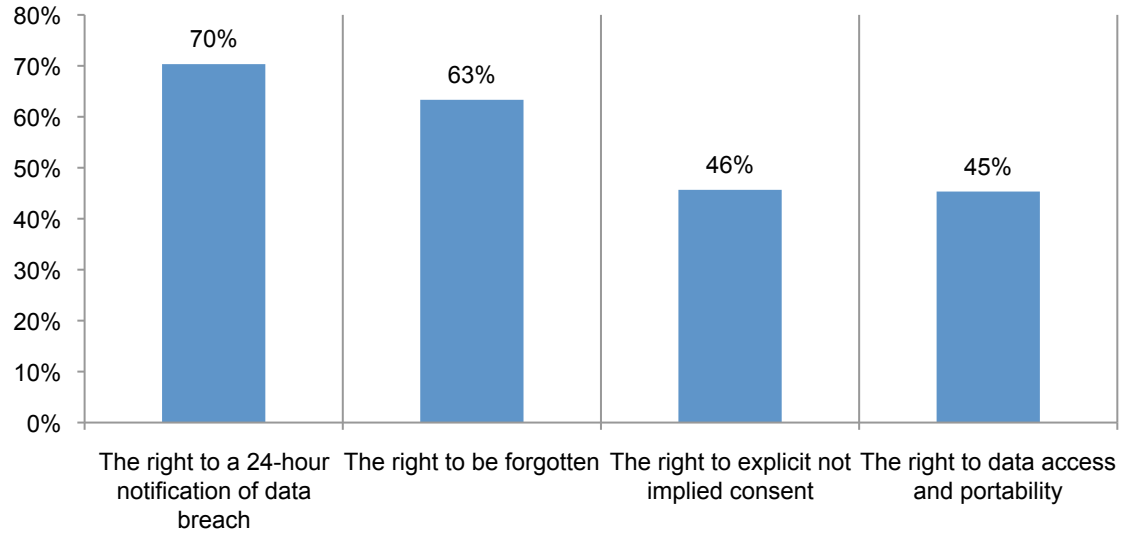
EU Privacy Laws

The study surveyed respondents in the UK, Germany and France to find out what they thought about the recently proposed EU guidelines on data protection report.[2] They were specifically asked about the following data subject rights:

- The right to a 24-hour notification of a data breach if the breach is likely to adversely affect the data subjects.
- The right to have their data erased also known as the right to be forgotten.
- The right of access to their data and the ability to make corrections.
- The right to explicit not implied consent and to object to direct marketing and profiling.
- The right to data portability. Where personal data is processed by electronic means and in a structure and commonly used format, the data subject is entitled to a copy.

The majority (63 percent) of respondents say the newly proposed privacy laws will have a very significant and significant impact on their overall business operations and compliance activities. According to Figure 17, the biggest impact will be the right to a 24-hour notification of data breach followed by the right to be forgotten.

Figure 17: The business impact of each consumer right
Very significant and significant response combined



[2]European Union Data Protection Reform: Proposal on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Brussels, January 25, 2012

Part 4. Methods

A sampling frame of 141,493 IT or IT security practitioners located in nine countries was selected as participants to this survey. As shown in Table 1, 5,743 respondents completed the survey. Screening removed 836 surveys and an additional 364 surveys that failed reliability checks were removed. The final sample was 4,774 surveys (or a 3.4 percent response rate).

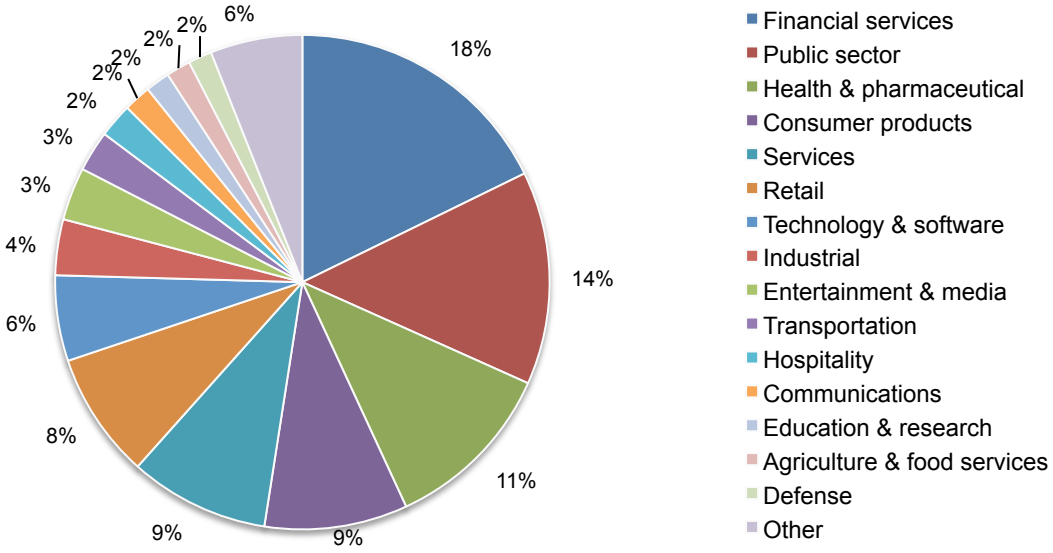
Table 1. Response	US	UK	AU	DE	FR	IN	JP	CH	BZ	Total
Sampling frame	18,172	15,667	13,560	16,551	13,889	17,019	16,574	14,555	15,506	141,493
Total returns	870	657	455	563	495	649	757	689	608	5,743
Total rejections	46	38	33	29	48	50	34	51	35	364
Screened	99	73	145	63	86	95	125	87	63	836
Final sample	712	527	485	606	451	554	577	438	424	4,774
Response rate	3.9%	3.4%	3.6%	3.7%	3.2%	3.3%	3.5%	3.0%	2.7%	3.4%

As noted in Table 2, the respondents' average (mean) experience in IT, or IT security is 9.77 years and a total of 5.79 years in their current position.

Table 2. Means	US	UK	AU	DE	FR	IN	JP	CH	BZ	Avg
Years in IT or IT security	9.88	9.56	9.55	10.49	10.20	9.78	10.08	8.07	9.90	9.77
Years in current position	5.60	5.57	5.86	6.17	5.85	6.62	5.16	4.80	6.55	5.79

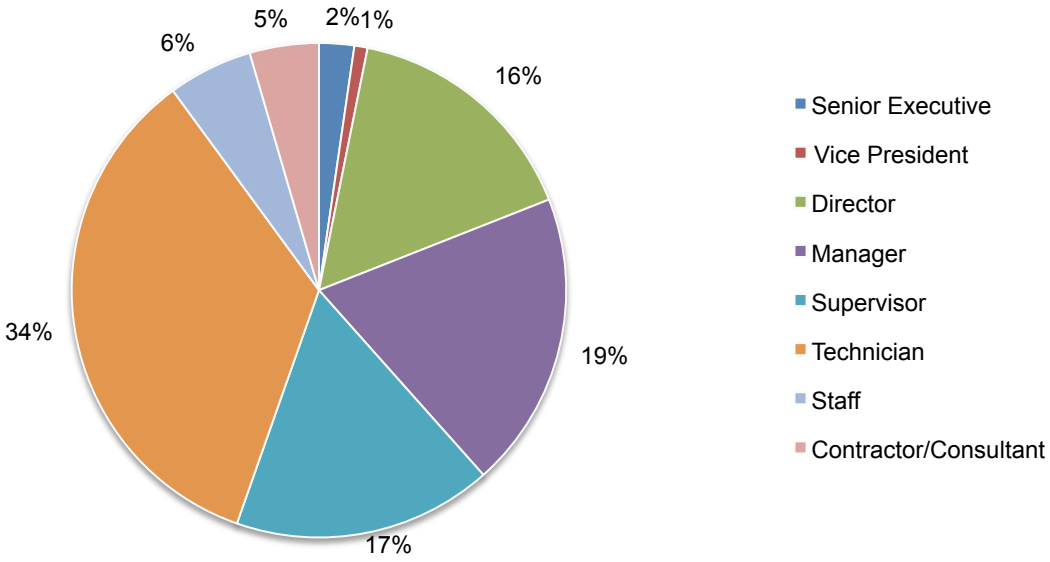
Pie Chart 1 reports the industry segments of respondents' organizations. This chart identifies financial services (18 percent) as the largest segment, followed by public sector (14 percent) and health & pharmaceutical (11 percent).

Pie Chart 1: Industry distribution of respondents' organizations



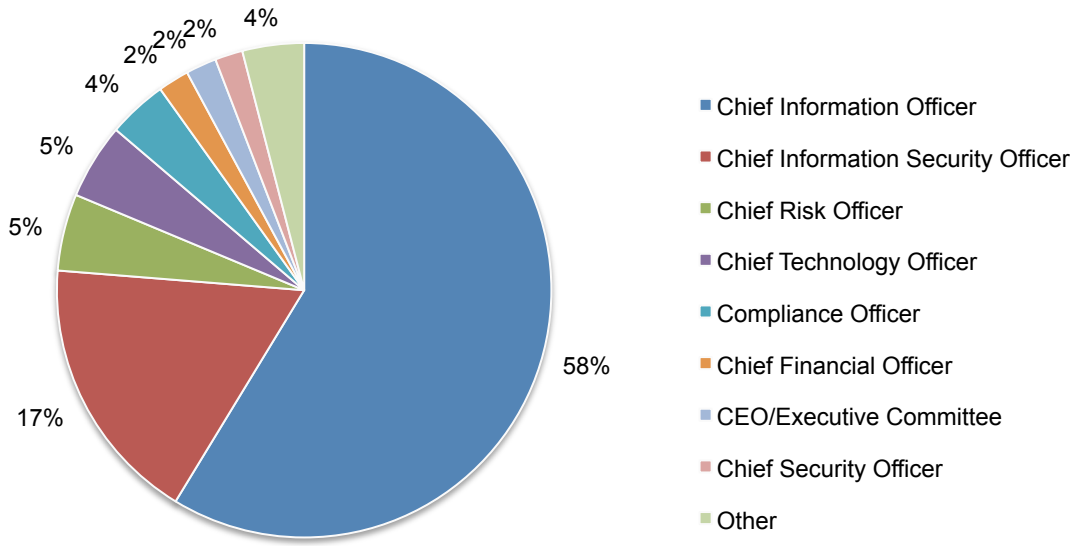
Pie Chart 2 reports the respondent's organizational level within participating organizations. By design, 55 percent of respondents are at or above the supervisory levels.

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



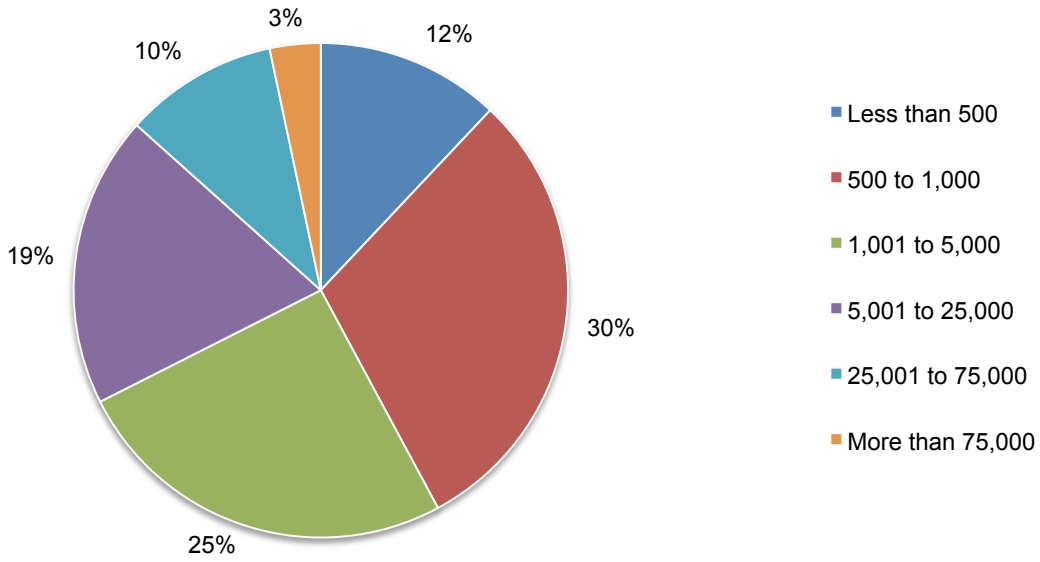
According to Pie Chart 3, 58 percent of respondents report directly to the Chief Information Officer and 17 percent report to the Chief Information Security Officer.

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



Fifty-seven percent of respondents are from organizations with a global headcount greater than 1,000 as shown in Pie Chart 4.

Pie Chart 4: Worldwide headcount



Part 5. 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. 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 consolidated by all nine countries. All survey responses were captured in the end of December 2012 through mid-January, 2013. Please note that Q16, 17 and 22 were removed because these survey items were not used in the final analysis.

Sample response	Total
Sampling frame	141,493
Total returns	5,743
Total rejections	364
Total returns before screening	5,379
Screened surveys	836
Final sample	4,774
Response rate	3.4%

Part 1. Screening

S1. How familiar are you with emerging network security technologies?	Total
Very familiar	1,655
Somewhat familiar	2,659
Not familiar	672
No knowledge (Stop)	457
Total	5,443

S2a. Please check the technologies that your organization presently uses or plans to use in the next 12 months.	Total
NGFW	2,490
IPS with reputation feeds	1,418
WAF	1,907
Other (please specify)	48
None of the above (Stop)	200
Total	6,063

S2b. If you selected one or more of these technologies, what is your organization's deployment strategy?	Total
To replace conventional network security technologies such as traditional firewalls	1,562
To augment conventional network security technologies such as traditional firewalls	1,759
No deployment strategy	1,453
Unsure (Stop)	179
Total	4,953

Final sample	4,774

Part 2. Attributions. Please rate the following statements using the five-point scale provided below each attribution about emerging network such technologies. Strongly agree and agree response combined.	Consolidated
Q3. Emerging network security technologies only address part of the cyber security threats facing my organization.	61%
Q4. In terms of protecting my organization, emerging network security technologies **fall short** of vendors' promises.	56%
Q5. My organization uses emerging network security technologies to heighten visibility to applications and the use of cloud services.	52%
Q6. My organization primarily uses emerging network security technologies to minimize the **inside-out** rather than **outside-in** security problem.	53%

Q7. Emerging network security technologies do not minimize attacks that bring down web applications or gratuitous Internet traffic.	48%
Q8. Emerging network security technologies used by my organization have high false positive rates.	57%
Q9. Emerging network security technologies used by my organization are dependent upon in-house personnel who possess the knowledge and expertise to operate them effectively.	49%
Q10. Securing web traffic is by far the biggest security concern for my organization.	56%
Q11. My organization prioritizes holistic rather than point solutions to managing cyber security threats.	41%

Part 3. Network security posture

Q12. Using the following 10-point scale, please rate the effectiveness of your organization's overall network security posture. Not effective =1 to very effective = 10.	Consolidated
1 to 2	18%
3 to 4	32%
5 to 6	27%
7 to 8	13%
9 to 10	9%
Total	100%
Extrapolated value	4.7

Q13. Using the following 10-point scale, please rate your organization's ability to quickly **detect** cyber attacks against networks? Poor =1 to excellent = 10.	Consolidated
1 to 2	20%
3 to 4	29%
5 to 6	26%
7 to 8	14%
9 to 10	10%
Total	100%
Extrapolated value	4.8

Q14. Using the following 10-point scale, please rate your organization's ability to **prevent** cyber attacks against networks? Poor = 1 to excellent = 10.	Consolidated
1 to 2	20%
3 to 4	31%
5 to 6	24%
7 to 8	14%
9 to 10	11%
Total	100%
Extrapolated value	4.8

Q15. Using the following 10-point scale, please rate your organization's ability to minimize **false positives** in identifying and containing cyber attacks against networks? Poor= 1 to excellent= 10.	Consolidated
1 to 2	18%
3 to 4	32%
5 to 6	25%
7 to 8	14%
9 to 10	10%
Total	100%
Extrapolated value	4.8

Q16a, Q16b and Q16c were removed

Q17 was removed

Q18. Please provide your opinion about the effectiveness of emerging network security technologies in minimizing the impact of each incident using the following scale. Very effective and effective combined.	Consolidated
Zero day attacks	36%
Exploit of existing software vulnerability less than 3 months old	41%
Exploit of existing software vulnerability greater than 3 months old	49%
SQL injection	34%
Botnet attacks	53%
Clickjacking	50%
Rootkits	61%
General malware	80%
Advanced malware	60%
Advanced persistent threats (APT)	53%
Hacktivism	35%

Q19. Where are you seeing the greatest rise of potential network security risk within your organization's IT environment? Please choose only your **top five** choices.	Consolidated
Our server environment	11%
Our data centers	12%
Within operating systems	16%
Across 3rd party applications	32%
Our PC desktop/laptop	23%
Mobile devices such as smart phones and tablets	58%
Removable media (USB sticks) and/or media (CDs, DVDs)	30%
Network infrastructure environment (gateway to endpoint)	27%
Malicious insider risk	52%
Negligent insider risk	48%
Cloud computing infrastructure and providers	53%
Virtual computing environments (servers, endpoints)	25%
Mobile/remote employees	46%
Lack of system connectivity/visibility	58%
Lack of organizational alignment	9%
Total	500%

Q20. Following is a list of network security priorities. In the context of your organization, please rate the relative priority of each item using the following scale. High priority response.	Consolidated
Minimizing false positives	38%
Increasing visibility to web traffic	78%
Increasing awareness about emerging threats	72%
Improving in-house knowledge and expertise	47%
Improving interoperability among network security technologies	46%
Reducing complexity in network security technologies	43%
Reducing the cost of deploying network security solutions	52%
Expediting the move from on-premise to cloud environments	63%
Enhancing network security awareness	50%
Average	54%

Q21. Using the following 10-point scale, please rate your organization's IT security personnel in terms of their knowledge and expertise in managing emerging network security technologies. Very low = 1 to very high = 10.	Consolidated
1 to 2	10%
3 to 4	16%
5 to 6	29%
7 to 8	19%
9 to 10	25%
Total	100%
Extrapolated value	6.2

Q22a, Q22b and Q22c were removed

Q23. What are the main reasons why your organization invested (or plans to invest in) emerging network security technologies? Please select all that apply.	Consolidated
Changing threat landscape	64%
Increase in the frequency of cyber attacks	27%
Increase in the sophistication of cyber attacks	65%
Existence of advance persistent threats (APT)	42%
Compliance with regulations and policies	43%
Need to prevent security breaches	26%
Other (please specify)	1%
Total	269%

Part 4. NGFW (only completed by respondents selecting NGFW in Q2a)

Q24. Of the following features, which of these do you consider to be most effective in security your organization's networks? Please rank order each one of these features from 1 = most effective to 5 = least effective.	Consolidated
Application control	3.14
Firewall	2.08
Intrusion prevention (IPS)	1.69
Virtual private network (VPN)	3.87
URL content filtering	4.21

Q25. Does your organization's NGFW suffer performance degradation when deploying the IPS feature?	Consolidated
Yes	53%
No	26%
Unsure	21%
Total	100%

Q26a. In using the application control feature in NGFW, how is it configured?	Consolidated
Monitoring and reporting only	53%
Security policy enforcement (allow/block)	23%
Corporate usage enforcement	46%
Restrict certain capabilities within applications	26%
Prevent bypassing of other security controls	23%
Total	170%

Q26b. If you **do not** have granularly configured application control, why?	Consolidated
Performance concerns about settings that are too granular	38%
Visibility is achieved without setting a high or very high setting	19%
Management sets the level	43%
Other (please specify)	1%
Total	100%

Part 5. WAF (only completed by respondents selecting WAF in Q2a)

Q27a. Does your organization deploy WAF in block mode?	Consolidated
Yes	42%
No	53%
Unsure	5%
Total	100%

Q27b. If **no**, why doesn't your organization deploy its WAF in block mode? Please select all that apply.	Consolidated
High false positives that sometimes blocks real customers	60%
Setting and updating blocking rules or policies are too difficult	54%
Insufficient time to decipher and handle blocked traffic	48%
Lack of expert personnel to decipher blocked traffic	36%
Other (please specify)	2%
Total	199%

Q27c. If **yes**, after setting up and configuring its WAF, how long did it take your organization before it turned on block mode?	Consolidated
Immediately	11%
Within a few hours	14%
Within a few days	26%
Within a few weeks	23%
Within a few months	15%
Within one year	7%
More than one year	4%
Total	100%

Q27d. How much IT/tech time does your organization spend each month updating rules or policies for **each** WAF?	Consolidated
Less than 1 hour	11%
1 to 4 hours	14%
5 to 8 hours	25%
1 to 3 days	24%
4 to 7 days	14%
1 to 2 weeks	9%
More than 2 weeks	4%
Total	100%

Part 6. Additional questions

Q28. In your opinion, is the blocking of IP addresses an effective security measure?	Consolidated
Yes	47%
No	44%
Unsure	8%
Total	100%

Q29a. Does your organization feel uncomfortable blocking IP addresses as a security measure?	Consolidated
Yes	47%
No	42%
Unsure	11%
Total	100%

Q29b. If yes, why does your organization feel uncomfortable blocking IP addresses as a security measure?	Consolidated
Possible false positives that block legitimate traffic	67%
Need to have a more granular identification method than simply IP addresses	51%
Other (please specify)	3%
Total	121%

Q30. What do you see as the most serious types of cyber attacks experienced by your company? Please select only three choices.	Consolidated
Viruses	12%
Malware	37%
Hacking	12%
Web-based attacks	62%
SQL injection	47%
Phishing	47%
Social engineering	21%
Denial of service	60%
Other (please specify)	2%
Total	300%

Q31. How many times has your company's network security been successfully breached over the past 12 months?	Consolidated
None	31%
1 time	26%
2 to 3 times	13%
4 to 5 times	11%
More than 5 times	10%
Cannot determine	9%
Total	100%
Extrapolated value	1.84

Special questions on newly proposed EU privacy laws

Q32. Based on the summary provided (above), in your opinion, how will this new proposed regulation impact your overall business operations and compliance activities?	Consolidated
Very significant and significant impact combined.	63%

Q33. What best describes your level of knowledge about the newly proposed EU privacy regulations?	Consolidated
Very knowledgeable	19%
Somewhat knowledgeable	61%
Little or no knowledge (Go to Part 7)	21%
Total	100%

Q34. Following are four notable consumer rights in the proposed EU privacy and data protection regulations. Please rate the **business impact** of each consumer right using the scale provided below the feature. Very significant and significant impact combined.	Consolidated
Q34a. The right to be forgotten.	63%
Q34b. The right to explicit not implied consent	46%
Q34c. The right to data access and portability	45%
Q34d. The right to a 24-hour notification of data breach	70%

Part 7. Your role and organization

D1. What organizational level best describes your current position?	Consolidated
Senior Executive	2%
Vice President	1%
Director	16%
Manager	19%
Supervisor	17%
Technician	34%
Staff	6%
Contractor/Consultant	5%
Other	0%
Total	100%

D2. Check the **Primary Person** you or your immediate supervisor reports to within the organization.	Consolidated
CEO/Executive Committee	2%
Chief Financial Officer	2%
General Counsel	1%
Chief Information Officer	58%
Chief Technology Officer	5%
Chief Information Security Officer	17%
Compliance Officer	4%
Chief Privacy Officer	0%
Human Resources VP	1%
Chief Security Officer	2%
Chief Risk Officer	5%
Other (please specify)	2%
Total	100%

Total years of relevant experience	Consolidated
D3a. Total years of IT or security experience	9.77
D3b. Total years in current position	5.79

D4. What industry best describes your organization's industry focus?	Consolidated
Agriculture & food services	2%
Communications	2%
Consumer products	9%
Defense	2%
Education & research	2%
Energy & utilities	1%
Entertainment & media	3%
Financial services	18%
Health & pharmaceutical	11%
Hospitality	2%
Industrial	4%
Public sector	14%
Retail	8%
Services	9%
Technology & software	6%
Transportation	3%
Other	5%
Total	100%

D5. What is the worldwide headcount of your organization?	Consolidated
Less than 500	12%
500 to 1,000	30%
1,001 to 5,000	25%
5,001 to 25,000	19%
25,001 to 75,000	10%
More than 75,000	3%
Total	100%
Extrapolated value	11,590

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.