Exposing the Cybersecurity Cracks: A Global Perspective

Part 2: Roadblocks, Refresh and Raising the Human Security IQ

Sponsored by Websense®

Independently conducted by Ponemon Institute LLC

Publication Date: July 17, 2014

Exposing the Cybersecurity Cracks
Part 2: Roadblocks, Refresh and Raising the Human Security IQ
July 17, 2014

Part 1. Introduction

Ponemon Institute is pleased to present the second report of its two-part study, *Exposing the Cybersecurity Cracks: A Global Perspective* sponsored by Websense. This is the second part of a two-part series on the challenges IT executives face in dealing with cyber risks. In this report it is revealed how better communication and information about cybersecurity, the right investment in skilled personnel and enabling technologies and the adoption of security measures will minimize the risk of current and emerging cyber threats.

The study surveyed 4,881 IT and IT security practitioners in the following 15 countries: Australia, Brazil, Canada, China, France, Germany, Hong Kong, India, Italy, Mexico, the Netherlands, Singapore, Sweden, United Kingdom and the United States. On average, participants in this research have 10 years of IT experience. This report covers the consolidated global findings[1].

The following are the most salient findings of this research:

Communication roadblocks are barriers to reducing the risk of a cyber attack. According to the findings, 31 percent of cyber security teams never speak with their executive team about cyber security. Of those that did, 23 percent spoke just annually and 19 percent spoke semi-annually. Just 1 percent spoke weekly.

Organizations want a security refresh. APT's and data exfiltration attacks rank as the top fears for IT security pros. These fears are probably due to concerns that their technology will not protect them. Many would like to see a complete security refresh of their solutions as they feel frequently disappointed with the level of protection their security solutions give them. In fact, 47 percent of respondents say their organizations have been very frequently or frequently disappointed in their security investments.

If they had the resources and opportunity, 29 percent of respondents would do a complete overhaul of their current enterprise security system if they had the resources and opportunity. Fifty-six percent say if their organizations had a data breach they would consider changing security vendors. Encouragingly, almost half (49 percent of respondents) say they are planning on making significant investments and adjustments to their cyber security defenses during the next 12 months.

Security professionals feel the top three events that would compel executive teams to allocate more money to cyber security initiates are: exfiltration of intellectual property (67 percent of respondents), data breach involving customer data (53 percent of respondents) and loss of revenues because of system downtime (49 percent of respondents).

The insider threat puts intellectual property and customer data at risk. Seventy-six percent of respondents say they personally know another security professional whose company had sensitive or confidential data stolen as a result of an insider threat. Sixty-three percent say the data stolen by the insider was intellectual property and customer information.

To mend the cracks, raise the human security IQ. Only thirty-eight percent of respondents believe their company is investing enough in skilled personnel and technologies to be effective in executing its cyber security objectives or mission. In fact, 48 percent of companies represented in this research do not provide cybersecurity education to their employees.

[1] Individual country reports of the research findings are also available.

Cyber threat modeling is considered important to managing cyber risk. Forty-two percent of respondents say their organizations have undergone a cyber threat modeling process in their present role. Of those that did, 94 percent found it to be important in terms of managing their cyber risk.

Very few companies take steps internally to deal with new and emerging threats. When there is awareness about a new cyber threat, the primary response is to reach out to outsiders such CERT, law enforcement and industry peers. An infrequent response is conducting assessments to determine vulnerability levels (11 percent) or having “fire drills” to determine readiness level (4 percent).

Part 2. Key Findings

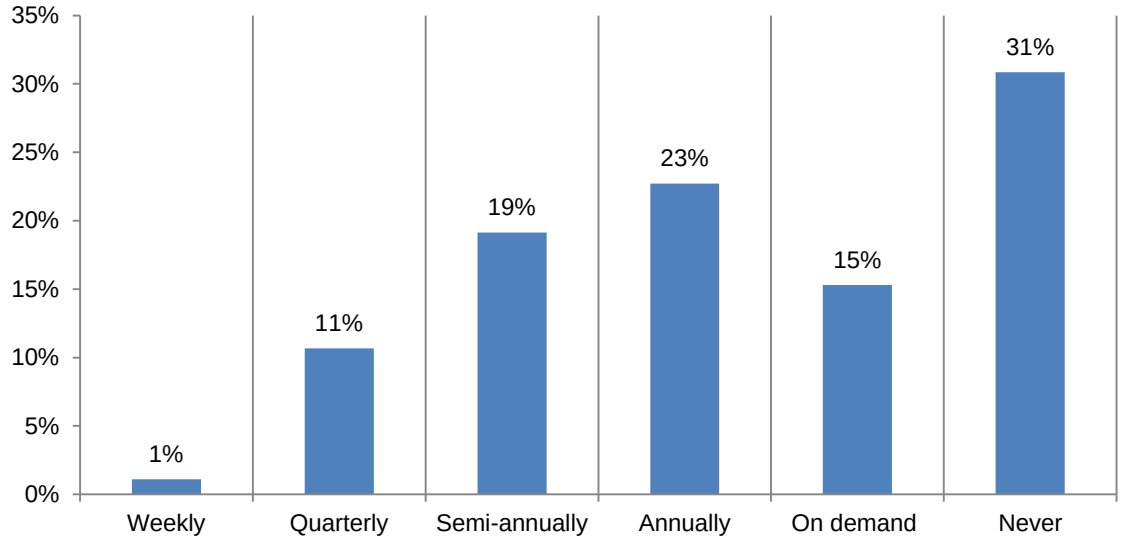
In this section we present an analysis of the consolidated findings. The complete audited findings are presented in the appendix of this report. We have organized the paper according to the following themes:

- **Communication roadblocks are barriers to reducing the risk of a cyber attack**
- **Organizations want a security refresh**
- **To mend the cracks, raise the human security IQ**

Communication roadblocks are barriers to reducing the risk of a cyber attack

Communication between the cyber security team and executives is rare. Figure 1 illustrates the reason why there is a disconnect between IT security and executives. Thirty-one percent say communication never occurs. Thirty-eight percent say they speak once a year or only when asked.

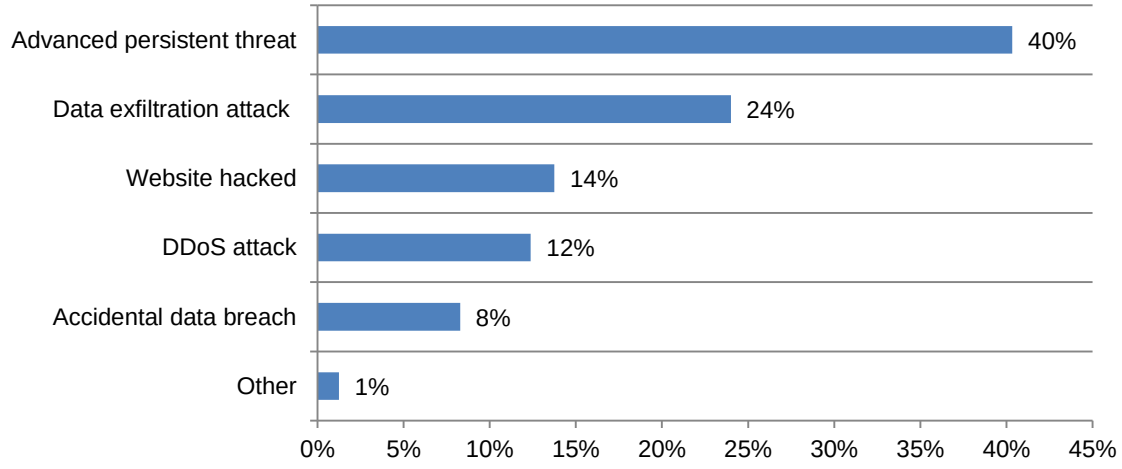
Figure 1: How often does your cyber security team speak with the executive team about cybersecurity?



Organizations want a security refresh

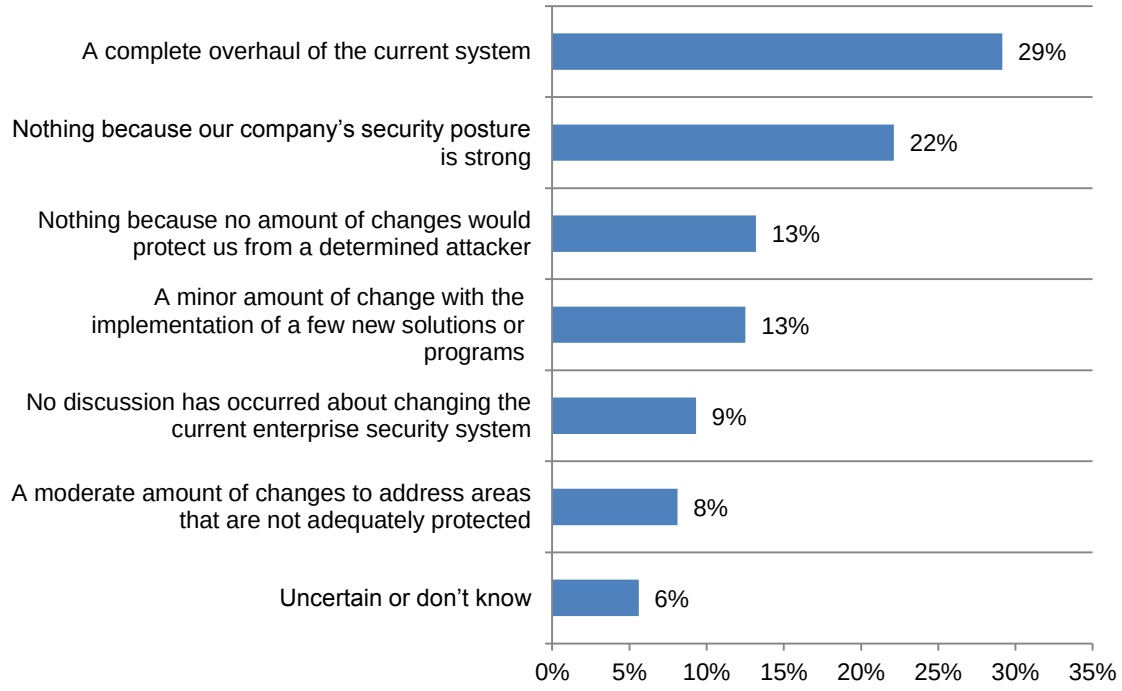
According to the findings of the research presented in the first report, 57 percent of cyber security professionals say they do not think their organization is protected from advanced cyber attacks. As shown in Figure 2, APT's and data exfiltration are among the top fears for cyber security professionals. This may be the result of technology solutions that do not provide enough protection.

Figure 2: As a security professional, what do you fear most?



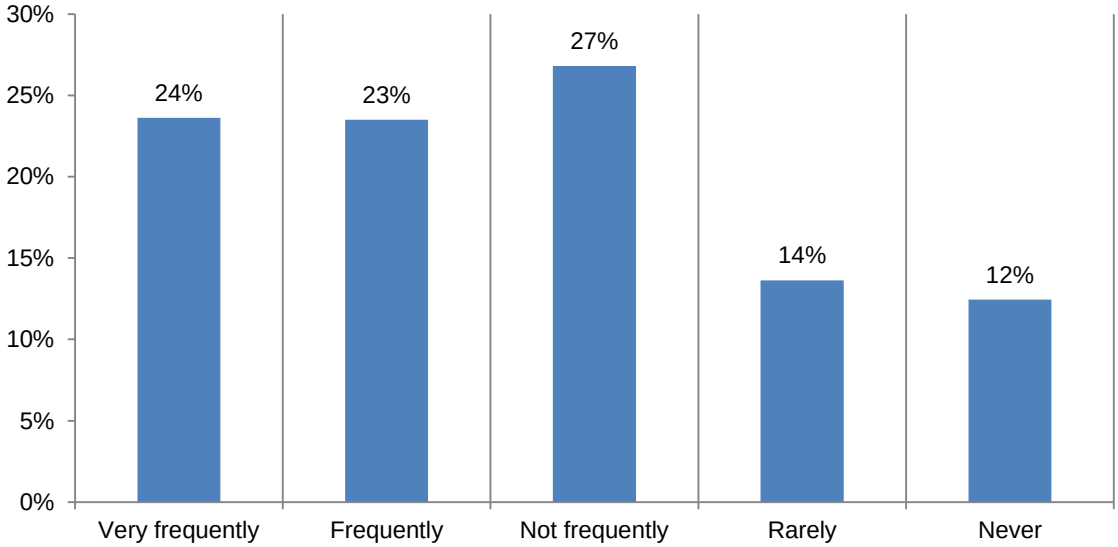
As shown in Figure 3, 29 percent of respondents would like to have a complete overhaul or refresh of their enterprise security systems. Many have felt disappointed with the protection solutions they have bought have given them.

Figure 3: What would the organization change about the current enterprise security system?



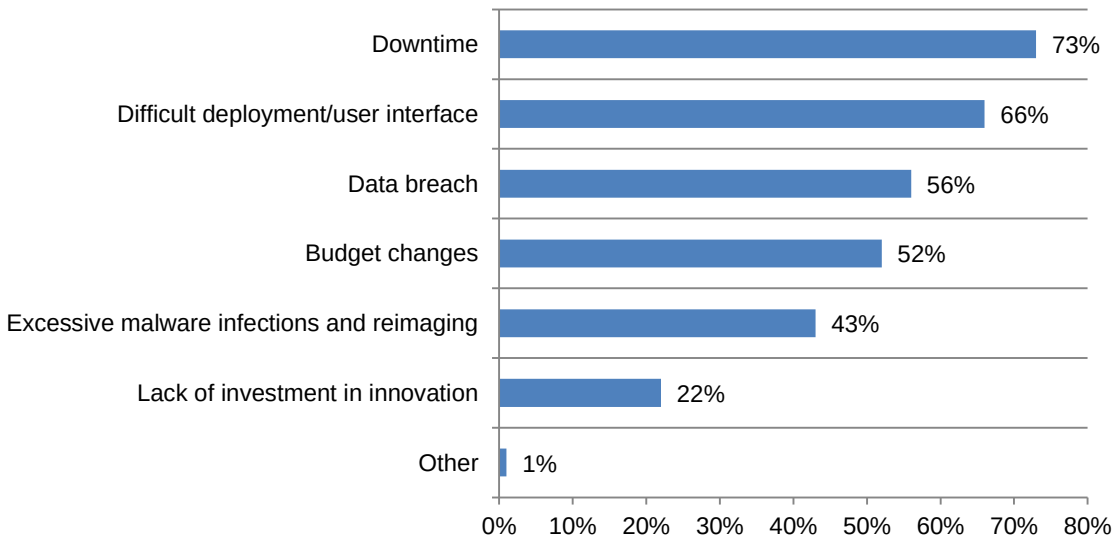
Can too much hype by security vendors lead to disappointing investments in technology? Fifty-eight percent say providers of security solutions hype the threats and risks companies face. Figure 4 shows that 47 percent of respondents say their company very frequently or frequently has purchased a security solution that was a disappointment.

Figure 4: Has your company ever procured an enabling security solution and then was disappointed with the protection it provided?



Downtime is the main reason to change security vendors. Respondents reveal the reasons they would change security vendors. As shown in Figure 5, downtime and difficult deployment/user interface are the top reasons that would trigger a change in security vendors. Fifty-six percent say a data breach would result in terminating a relationship with a security vendor.

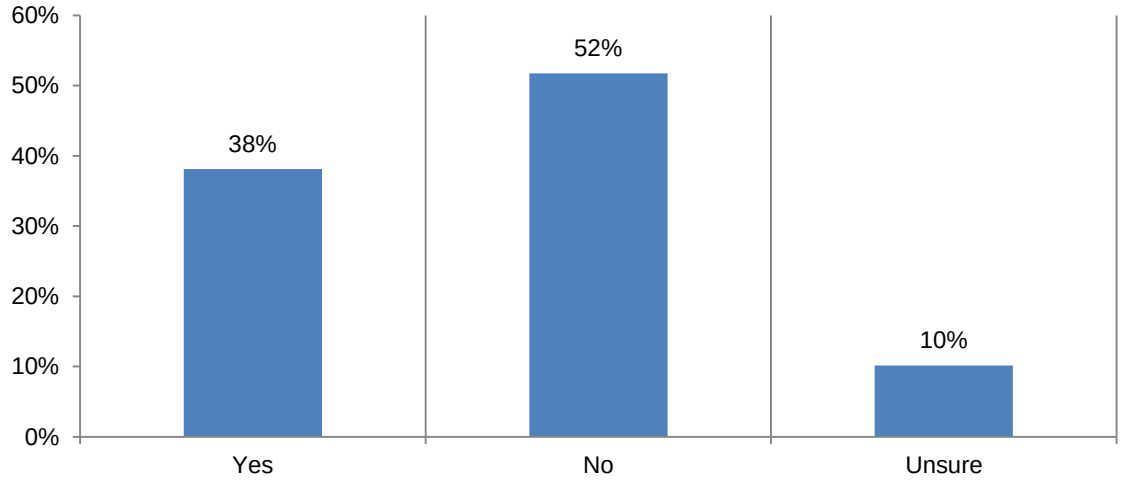
Figure 5: What would trigger your company to change security vendors?
More than one response permitted



Cybersecurity professionals want more funding to combat threats. To deal with the challenging and dynamic threat landscape, organizations need to have the intelligence to anticipate, identify and reduce the threats.

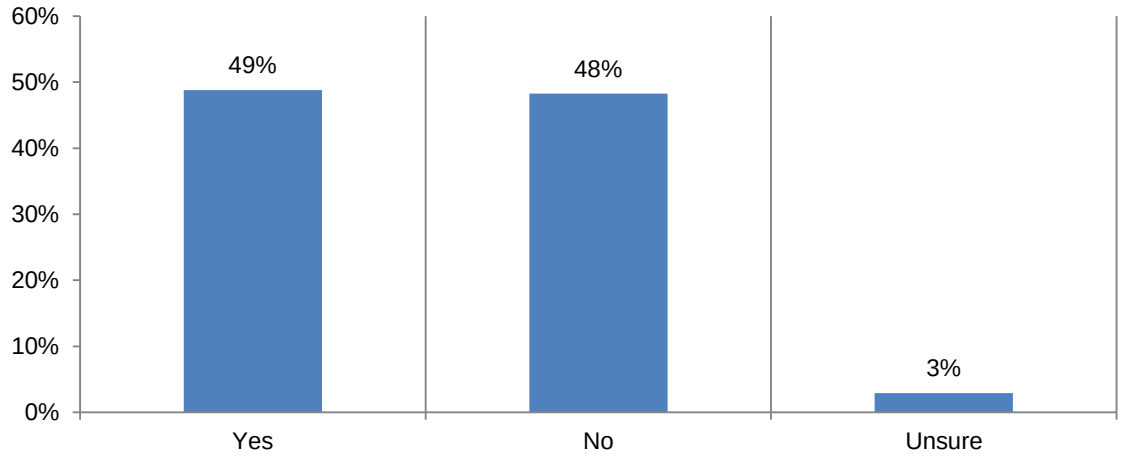
Figure 6 shows that security professionals do not believe they are getting the right level of investment to be able to achieve their cyber security objectives and mission. Only 38 percent say their companies invest enough in skilled personnel and technologies to be effective in executing its cybersecurity objectives or mission. Sixty-two percent of respondents say it is not enough or they are unsure about the level of investment.

Figure 6: Does your company invest in skilled personnel and technologies for cyber security defenses?



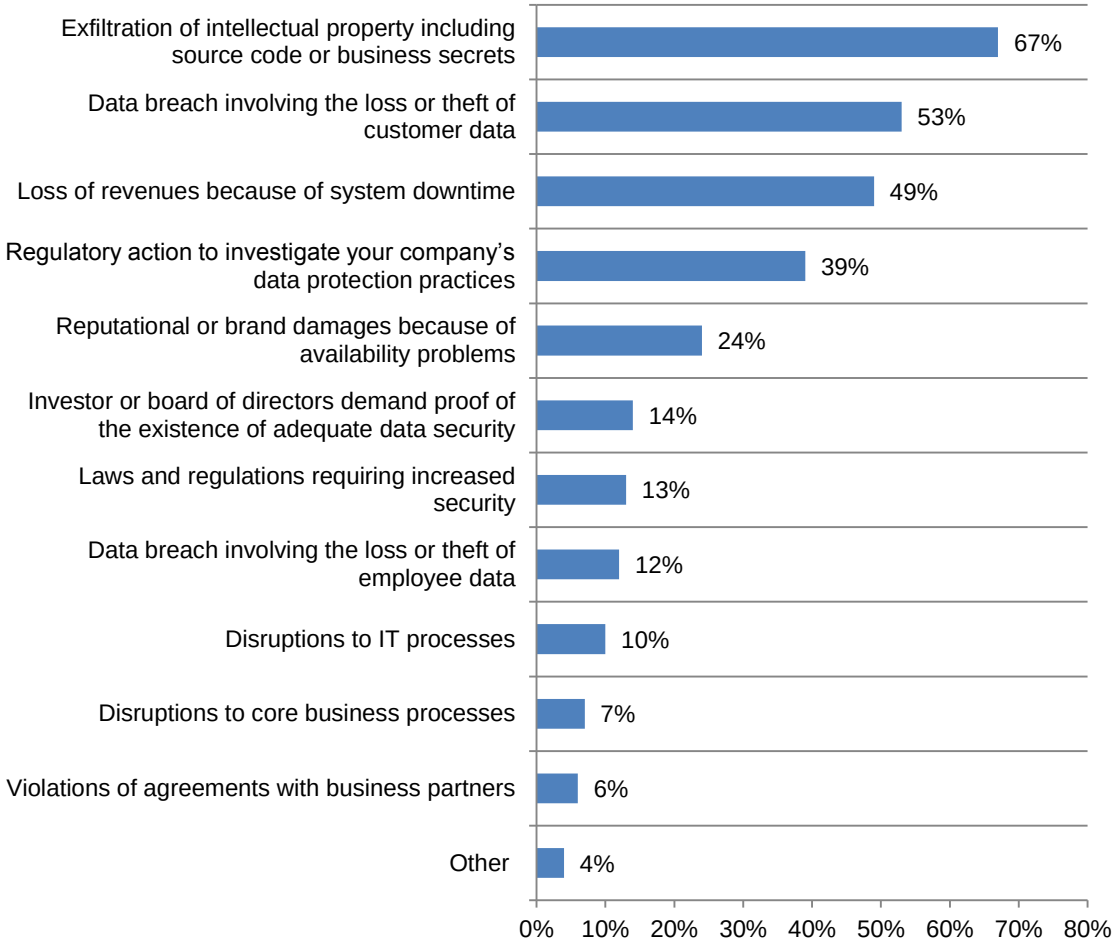
Future investment plans are encouraging. With the acknowledgement of the risks facing their organizations, just under half (49 percent of respondents) say there is a plan to make significant investments and/or adjustments to its cybersecurity defenses over the next 12 months, according to Figure 7.

Figure 7: Is your company planning to make significant investments and/or adjustments to its cyber security defenses over the next 12 months?



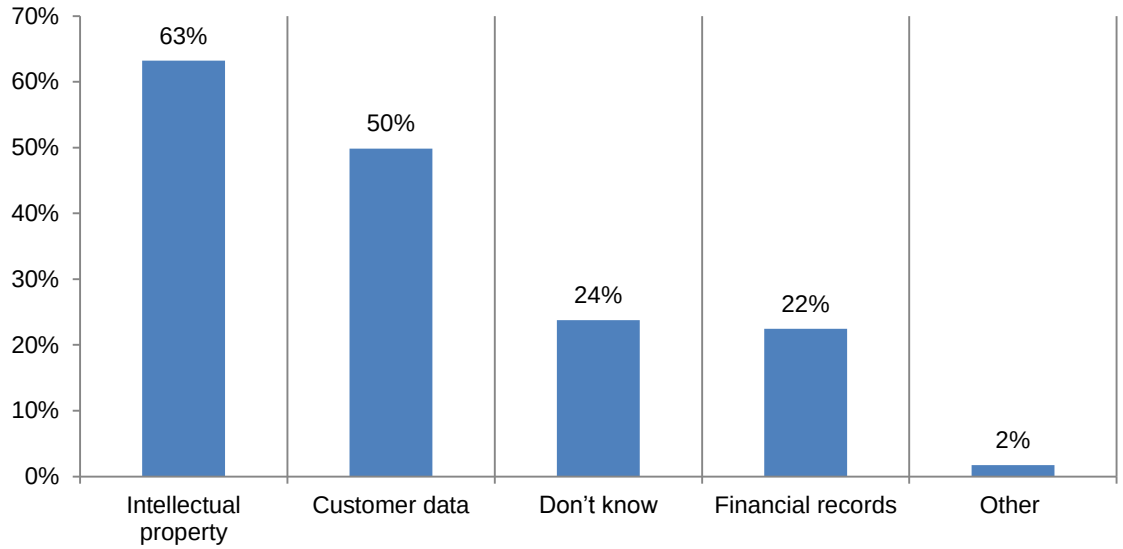
How can IT executives get more funding for cyber security initiatives? According to Figure 8, security professionals feel the top three events that would compel executive teams to allocate more money to cyber security initiates are: exfiltration of intellectual property (67 percent of respondents), data breach involving customer data (53 percent of respondents) and loss of revenues because of system downtime (49 percent of respondents).

Figure 8: What events would compel your company's executive team to allocate more money to cyber security initiatives?



The insider threat puts intellectual property and customer data at risk. Seventy-six percent of respondents say they personally know another security professional whose company had sensitive or confidential data stolen as a result of an insider threat. As shown in Figure 9, 63 percent of respondents who are aware of an insider attack say the data stolen was intellectual property and customer information.

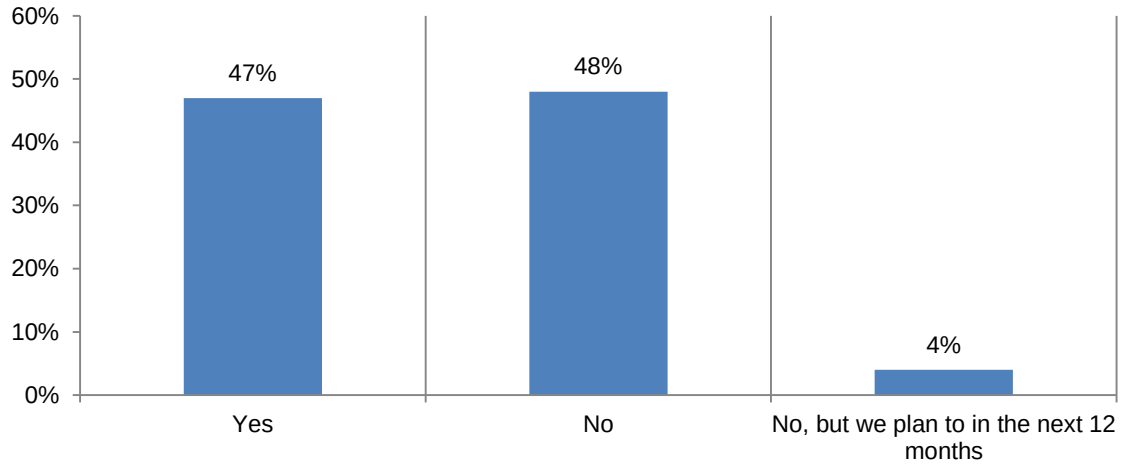
Figure 9: Confidential data stolen by an insider



To mend the cracks, raise the human security IQ.

Companies require security intelligence and user education to try and close cybersecurity gaps. As shown in Figure 10, 51 percent of respondents say they now provide cybersecurity education to their employees or plan to in the next 12 months. Less than half (48 percent of respondents) say their organizations do not offer such training. Such education is critical to making employees aware of the threats facing their organization and the importance of adhering to security policies and procedures established by their organizations.

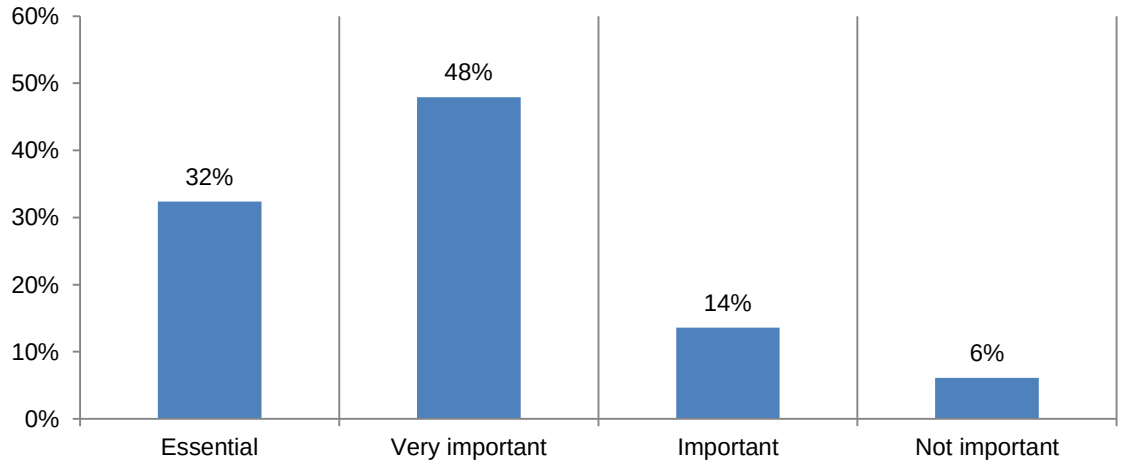
Figure 10: Do you provide cybersecurity education to your employees?



Cyber threat modeling process should be part of an organization's cyber defenses. Forty-two percent of respondents say their organizations have undergone a cyber threat modeling process in their roles. Fifty-eight percent say they have not engaged in cyber threat modeling (55 percent of respondents) or they are unsure (3 percent of respondents).

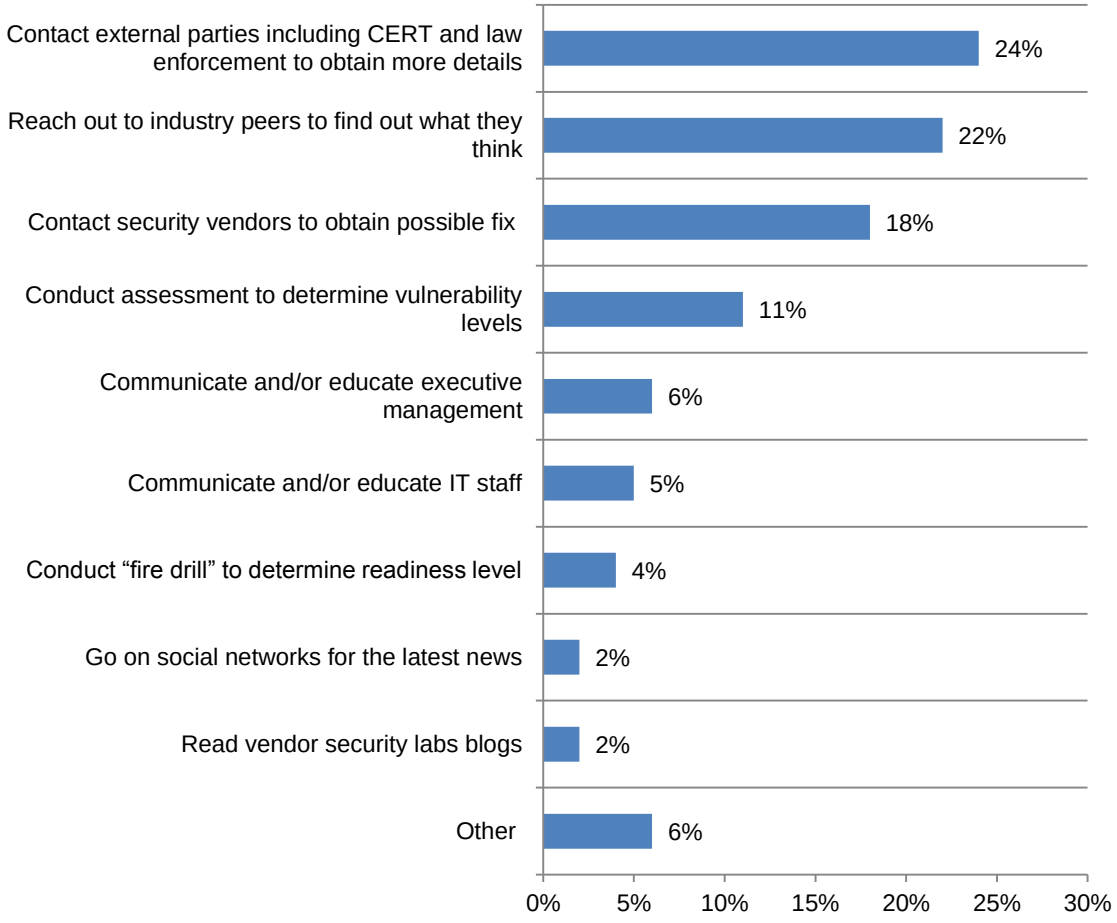
As shown in Figure 11, of those organizations that did have a cyber threat modeling process, 80 percent say it is essential or very important to managing cyber risk.

Figure 11: How important is cyber threat modeling to manage cyber risk?



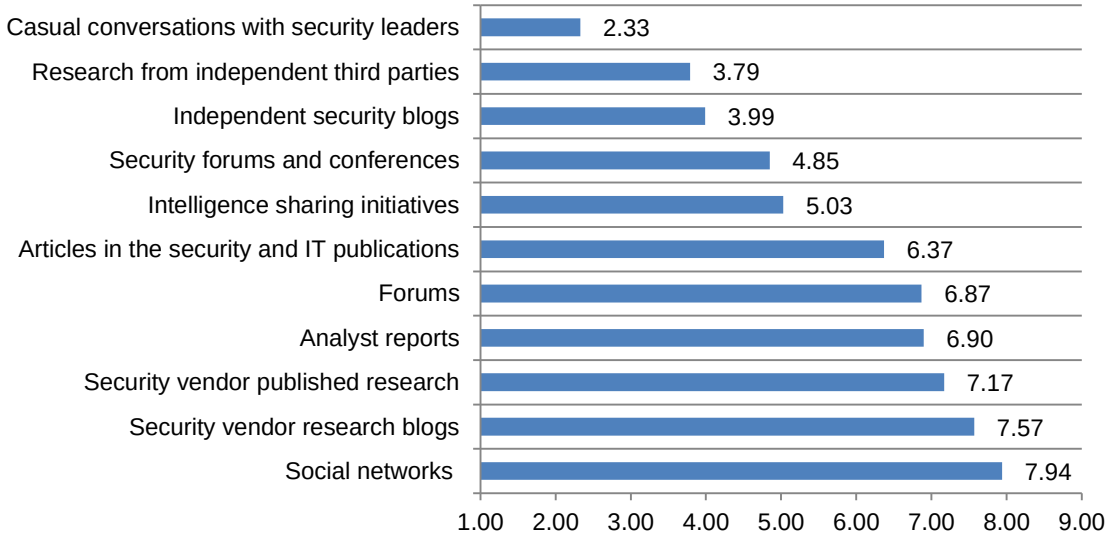
Very few companies take steps internally to deal with new and emerging threats. As shown in Figure 12, when there is awareness about a new cyber threat, the primary response is to reach out to outsiders such as CERT, law enforcement and industry peers. An infrequent response is conducting assessments to determine vulnerability levels (11 percent) or having "fire drills" to determine readiness levels (4 percent).

Figure 12: What's the first thing you do when you hear about a new or emerging cyber threat?



How do IT practitioners keep up-to-date about cyber threats? To keep informed and current about the threat landscape, respondents most often rely upon casual conversations with security leaders, research from independent third parties and security blogs, as shown in Figure 13.

Figure 13: How are you keeping up to date with the threat landscape?
1=most important to 11=least important

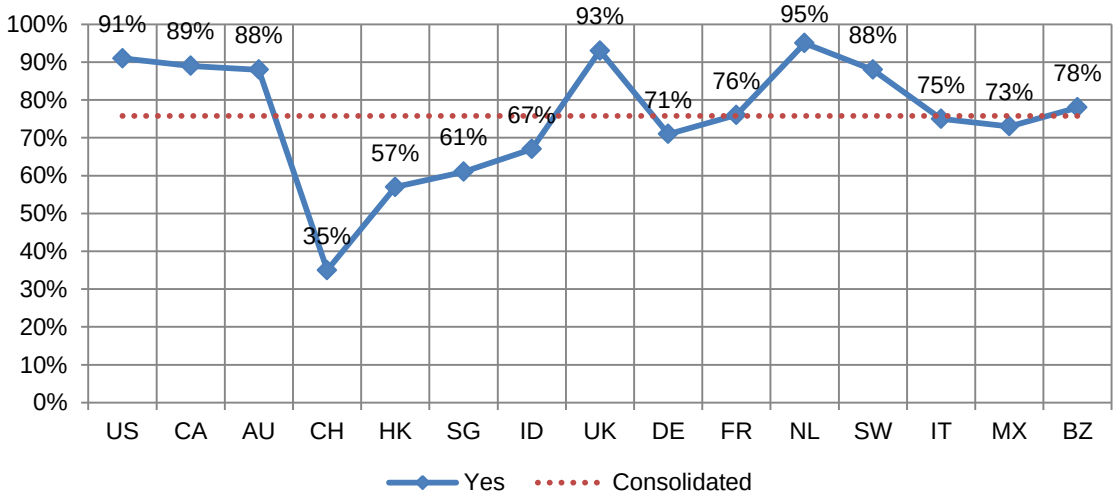


Part 3. Country Comparisons

In this section, we present the country differences to some of the most salient findings. For more information, individual country reports are available.

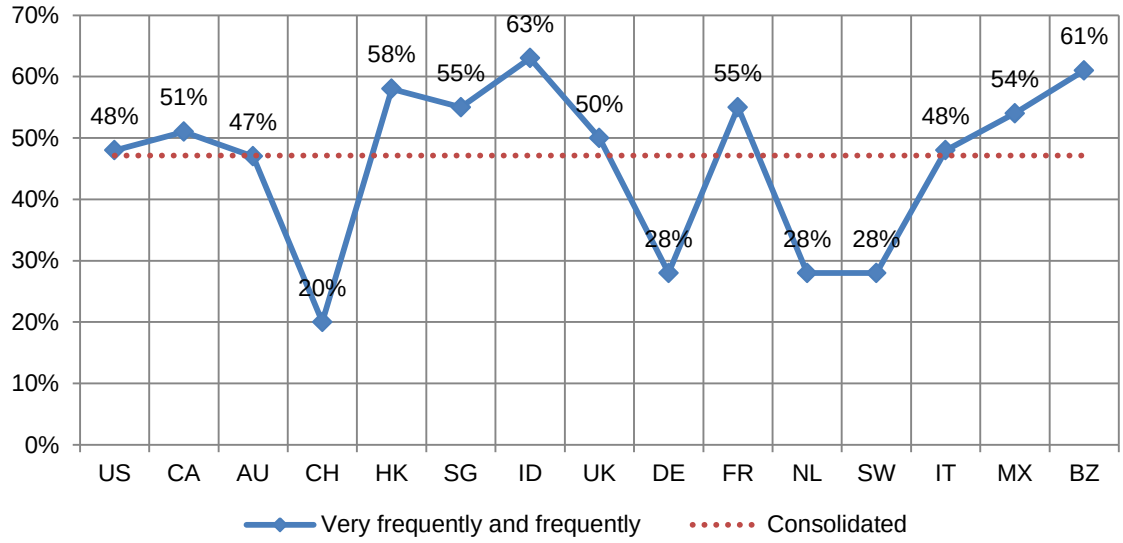
The insider threat varies significantly among countries. As shown in Figure 14, the insider threat seems to be most prevalent in the Netherlands, UK and U.S. Ninety-five percent of respondents in the Netherlands say they are personally aware of an insider attack followed by 93 percent in the UK and 91 percent in the U.S. Findings from respondents in China indicate organizations in that country have the lowest insider threat.

Figure 14: Do you personally know another security professional whose company had sensitive data stolen as a result of an insider threat?



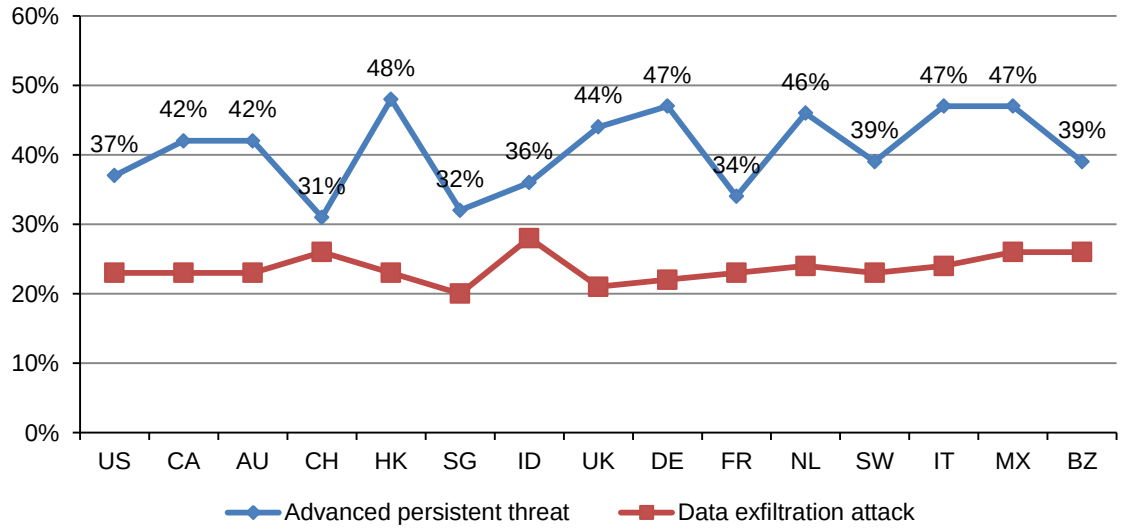
Respondents in certain countries have a higher rate of disappointment in their security solutions. According to Figure 15, the greatest disappointment in an investment in security solutions exists in India followed by Brazil (63 percent and 61 percent of respondents, respectively). The most satisfaction with security vendors occur in China, Germany the Netherlands and Sweden.

Figure 15: Has your company ever procured an enabling security solution and then was disappointed with the protection it provided?
Very frequently and frequently responses combined



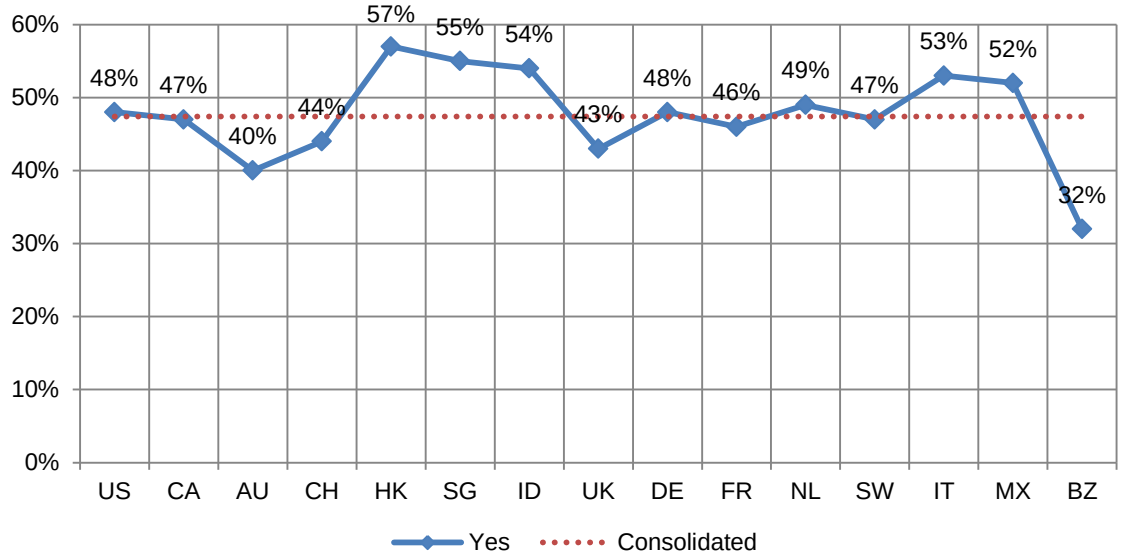
The biggest security concerns are APTs and data exfiltration attacks. When asked to select the security threats they worry most about, respondents agree that they are APTs and data exfiltration attacks. Respondents in Hong Kong, Germany, Italy and Mexico have the greatest concern about APTS. Singapore and China are least concerned, as shown in Figure 16. India and China worry most about data exfiltration attacks.

Figure 16: Security professionals are most worried about APTs and data exfiltration attacks



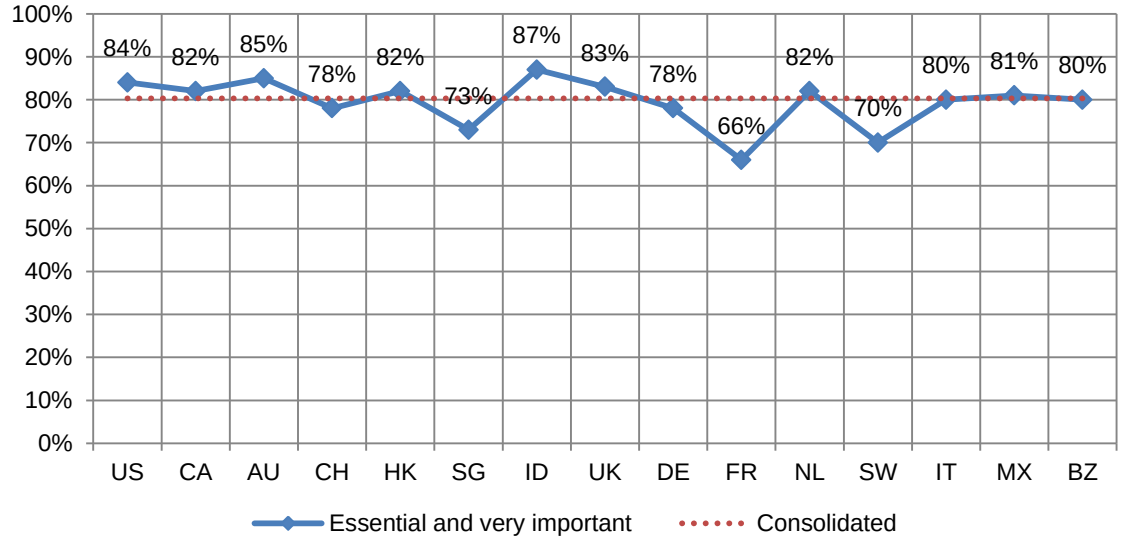
What is the global state of cybersecurity education? As shown in Figure 17, certain countries are more advanced in educating employees about cybersecurity. The majority of respondents in Hong Kong, Singapore, India, Italy and Mexico say their organizations provide cybersecurity training and awareness. Brazil, Australia, UK and China have the lowest level of respondents who say training exists in their organizations

Figure 17: Do you provide cybersecurity education to your employees?
Yes responses



Cyber threat modeling is important to managing cyber risk. An effective approach to reducing the risk of a cyber attack is to conduct cyber threat modeling exercises. As shown in Figure 18, the countries with the highest belief that it is essential or very important are India, Australia and the U.S.

Figure 18: How important is the cyber threat modeling process in terms of managing cyber risk?
Essential and very important response combined



Conclusion

The findings of this study expose the cracks in cybersecurity defenses that exist for many organizations. How can companies better manage the cyber attacks targeting their sensitive and confidential information? The following are some recommendations:

- Eliminate the uncertainty of cyber risks. Invest in technologies that provide visibility and details about high-risk behavior, attempted attacks and the consequences of a successful on your organization.
- Improve access to better threat intelligence and real-time defenses.
- Deploy an all-encompassing defense strategy that incorporates web and email channels, including SSL/TLS communications. Avoid focusing on just one channel. Rather, examine all the channels used to interact with information.
- Assess security solution capabilities and deployments against a comprehensive kill chain model to eliminate gaps and minimize excessive overlap. Expand beyond defenses overly dependent upon identifying an attack at only the “malware” delivery stage.
- Create security education and awareness programs that focus on the seriousness of cyber attacks and the importance of reducing high-risk behaviors.

Methods

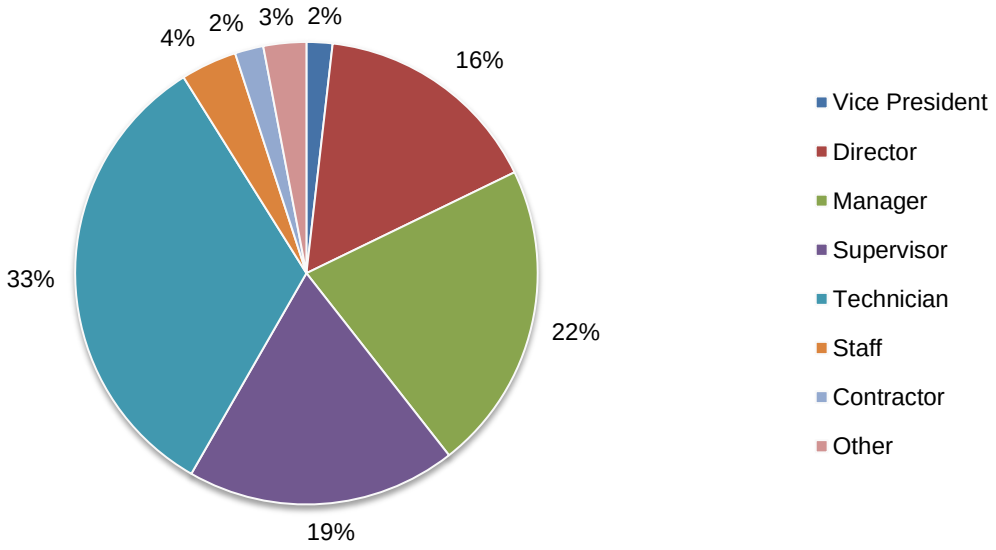
Table 1 reports the sample response for 15 countries. A total of 160,534 IT and IT security practitioners located in 15 countries were invited to participate in this global study. A total of 5,244 respondents returned the survey. Tests for reliability and screening removed 363 surveys. The final combined sample was 4,881 surveys, thus yielding a 3.0 percent response rate.

Table 1. Survey response

Countries	Abbreviations	Sampling frame	Total survey returns	Screened or rejected	Final sample	Response rate
Australia	AU	5,570	214	14	200	3.6%
Brazil	BZ	15,996	417	25	392	2.5%
Canada	CA	7,300	249	13	236	3.2%
China	CH	11,901	409	42	367	3.1%
France	FR	11,503	348	22	326	2.8%
Germany	DE	12,230	445	30	415	3.4%
Hong Kong	HK	4,693	219	18	201	4.3%
India	ID	23,677	583	38	545	2.3%
Italy	IT	6,900	269	19	250	3.6%
Mexico	MX	12,509	392	33	359	2.9%
Netherlands	NL	8,901	300	13	287	3.2%
Singapore	SG	3,659	200	12	188	5.1%
Sweden	SW	2,555	120	5	115	4.5%
United Kingdom	UK	11,580	422	31	391	3.4%
United States	US	21,560	657	48	609	2.8%
Consolidated	--	160,534	5,244	363	4,881	3.0%

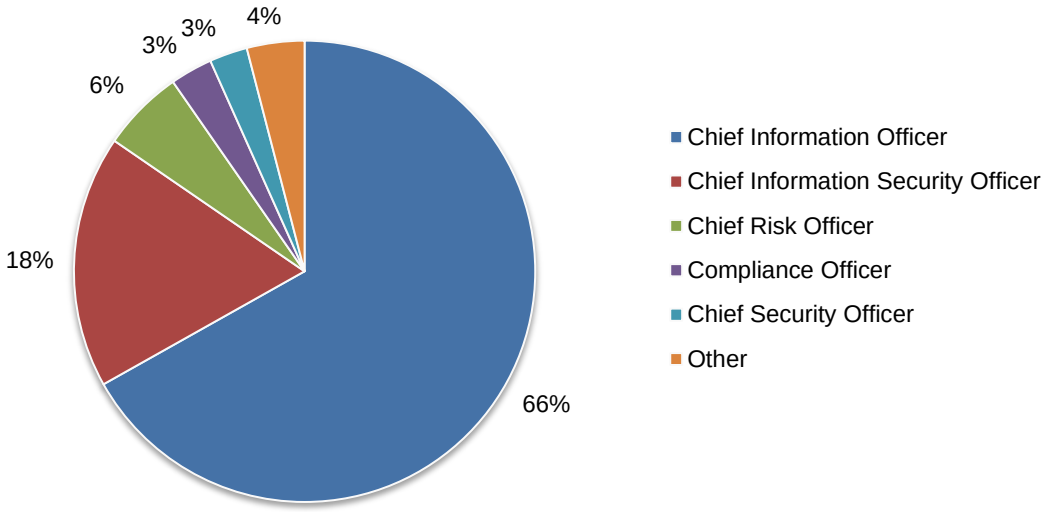
Pie Chart 1 reports the respondent's organizational level within participating organizations. By design, 59 percent of respondents are at or above the supervisory levels.

Pie Chart 1: What organizational level best describes your current position?
Consolidated results for 15 countries



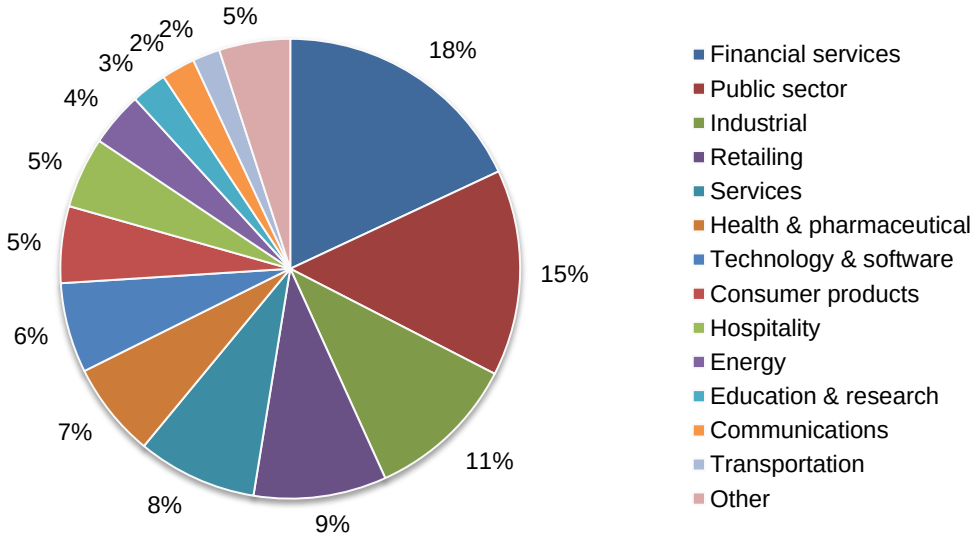
According to Pie Chart 2, 66 percent of respondents report directly to the chief information officer and 18 percent report to the chief information security officer.

Pie Chart 2: Primary Person you or your IT security leader reports to
Consolidated results for 15 countries



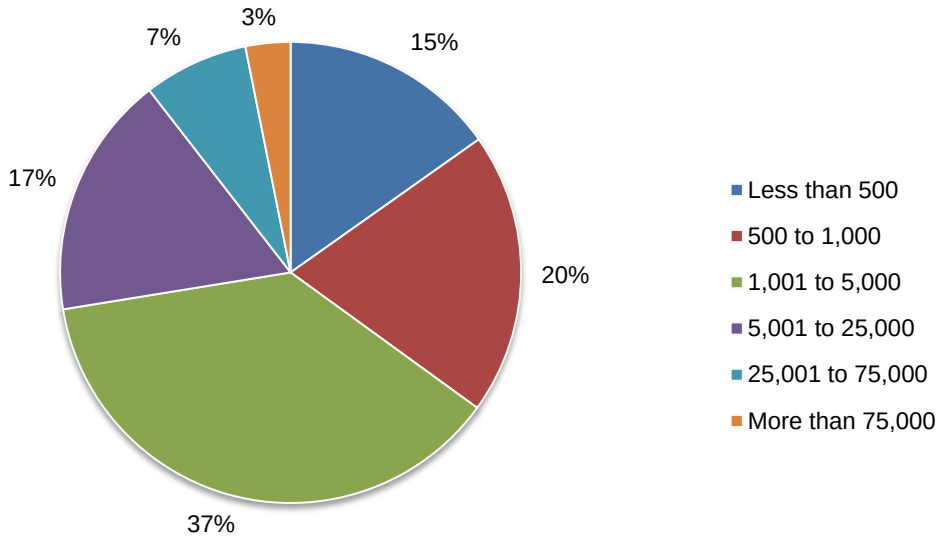
Pie Chart 3 reports the industry segments of respondents' organizations. This chart identifies financial services (18 percent) as the largest segment, followed by public sector (15 percent) and industrial (11 percent).

Pie Chart 3: What industry best describes your organization's industry focus?
Consolidated results for 15 countries



Pie Chart 4 reveals the worldwide headcount of the respondent's organization. Sixty-four percent of respondents are from organizations with a global headcount greater than 1,000.

Pie Chart 4: Organization's worldwide headcount
Consolidated results for 15 countries



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. Surveys were sent to a representative sample of individuals in 15 countries, 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 their underlying beliefs from those who responded to our survey request.

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 to all survey questions contained in this study. All survey responses were captured in November 2013.

Survey response	Total
Sampling frame	160534
Total survey returns	5244
Screened and rejected surveys	363
Final sample	4881
Response rate	3.0%

Part 1. Screening

S1. How familiar are you with the cyber threats facing your company?	Total
Very familiar	48%
Familiar	52%
Not familiar (stop)	0%
Total	100%

S2. How are you involved in your company's cyber threat intelligence activities? Please select all that apply.	Total
User of cyber threat intelligence	73%
Gatherer of cyber threat intelligence	49%
Analyzer of cyber threat intelligence	45%
Executive or manager in-charge of threat intelligence activities	35%
None of these roles (stop)	0%
Total	202%

Part 2: Attack intelligence

Q10a. Do you personally know another security professional whose company had sensitive or confidential data stolen as a result of an insider threat (i.e., exfiltration)?	Total
Yes	76%
No	24%
Total	100%

Q10b. If yes, what confidential data was stolen by the insider?	Total
Financial records	22%
Customer data	50%
Intellectual property	63%
Don't know	24%
Other (please list)	2%
Total	161%

Q11. Is your company planning to make significant investments and/or adjustments to its cyber security defenses over the next 12 months?	Total
Yes	49%
No	48%
Unsure	3%
Total	100%

Q13. Has your company ever procured an enabling security solution and then was disappointed with the protection it provided?	Total
Very frequently	24%
Frequently	23%
Not frequently	27%
Rarely	14%
Never	12%
Total	100%

Q14. If your company had the resources and opportunity, what would it change about the current enterprise security system?	Total
A complete overhaul of the current system	29%
A moderate amount of changes to address areas that are not adequately protected	8%
A minor amount of change with the implementation of a few new solutions or programs	13%
Nothing because our company's security posture is strong	22%
Nothing because no amount of changes would protect us from a determined attacker	13%
No discussion has occurred about changing the current enterprise security system	9%
Uncertain or don't know	6%
Total	100%

Part 3. Triggers for change

Q15. Do you think the providers of security solutions hype the threats and risks companies face?	Total
Yes	58%
No	35%
Unsure	7%
Total	100%

Q19. How often does your cyber security team speak with the executive team about cyber security?	Total
Daily	0%
Weekly	1%
Quarterly	11%
Semi-annually	19%
Annually	23%
On demand (only when asked)	15%
Never	31%
Total	100%

Q20. What type of events would compel your company's executive team to allocate more money to cyber security initiatives? Please select three choices.	Total
Investor or board of directors demand proof of the existence of adequate data security	14%
Data breach involving the loss or theft of customer data	53%
Data breach involving the loss or theft of employee data	12%
Exfiltration of intellectual property including source code or business secrets	67%
Laws and regulations requiring increased security	13%
Regulatory action to investigate your company's data protection practices	39%
Disruptions to core business processes	7%
Disruptions to IT processes (resulting in downtime)	10%
Loss of revenues because of system downtime	49%
Reputational or brand damages because of availability problems	24%
Violations of agreements with business partners	6%
Other (please specify)	4%
Total	300%

Q21. As a security professional, what do you fear most?	Total
Advanced persistent threat	40%
Data exfiltration attack	24%
Accidental data breach	8%
Website hacked	14%
DDoS attack	12%
Other	1%
Total	100%

Q22. What would trigger your company to change security vendors?	Total
Data breach	56%
Excessive malware infections and reimaging	43%
Difficult deployment/user interface	66%
Lack of investment in innovation	22%
Downtime	73%
Budget changes	52%
Other	1%
Total	310%

Q23. Do you provide cybersecurity education to your employees?	Total
Yes	47%
No	48%
No, but we plan to in the next 12 months	4%
Total	100%

Q24. Does your company invest enough in skilled personnel and technologies to be effective in executing its cyber security objectives or mission?	Total
Yes	38%
No	52%
Unsure	10%
Total	100%

Q25. What's the first thing you do when you hear about a new or emerging cyber threat?	Total
Reach out to industry peers to find out what they think	22%
Read vendor security labs blogs	2%
Conduct assessment to determine vulnerability levels	11%
Communicate and/or educate IT staff	5%
Communicate and/or educate executive management	6%
Contact security vendors to obtain possible fix (patch)	18%
Conduct "fire drill" to determine readiness level	4%
Contact external parties including CERT and law enforcement to obtain more details	24%
Go on social networks for the latest news	2%
Visit favorite media outlets and search for stories about the threat	1%
Nothing (no specific action taken)	1%
Other (please specify)	4%
Total	100%

Q26. How are you keeping up to date with the threat landscape? Please rank in order of importance (1=most important and 11=least important)	Total
Independent security blogs	3.99
Security vendor research blogs	7.57
Security vendor published research	7.17
Analyst reports	6.90
Articles in the security and IT publications	6.37
Casual conversations with security leaders	2.33
Security forums and conferences	4.85
Intelligence sharing initiatives (including CIRT)	5.03
Social networks (Facebook, Twitter, LinkedIn, etc.)	7.94
Forums	6.87
Research from independent third parties	3.79

Q27a. Have you gone through the cyber threat modeling process in your present role?	Total
Yes	42%
No	55%
Unsure	3%
Total	100%

Q27b. If yes, how important is the cyber threat modeling process in terms of managing cyber risk?	Total
Essential	32%
Very important	48%
Important	14%
Not important	6%
Total	100%

Part 4. Organizational characteristics & respondent demographics	
D1. What organizational level best describes your current position?	Total
Senior Executive	1%
Vice President	2%
Director	16%
Manager	22%
Supervisor	19%
Technician	33%
Staff	4%
Contractor	2%
Other	3%
Total	100%

D2. Total years of relevant experience	Total
Total years of IT or security experience	9.66
Total years in current position	4.85

D3. Check the **Primary Person** you or your IT security leader reports to within the organization.	Total
CEO/Executive Committee	0%
Chief Financial Officer	1%
General Counsel	0%
Chief Information Officer	66%
Chief Information Security Officer	18%
Compliance Officer	3%
Human Resources VP	0%
Chief Security Officer	3%
Chief Risk Officer	6%
Other	3%
Total	100%

D4. What industry best describes your organization's industry focus?	Total
Agriculture & food services	1%
Communications	2%
Consumer products	5%
Defense & aerospace	1%
Education & research	3%
Energy	4%
Entertainment & media	1%
Financial services	18%
Health & pharmaceutical	7%
Hospitality	5%
Industrial	11%
Public sector	15%
Retailing	9%
Services	8%
Technology & software	6%
Transportation	2%
Other	2%
Total	100%

D5. What is the worldwide headcount of your organization?	Total
Less than 500	15%
500 to 1,000	20%
1,001 to 5,000	37%
5,001 to 25,000	17%
25,001 to 75,000	7%
More than 75,000	3%
Total	100%

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 organization identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.