

The Rise of Nation State Attacks

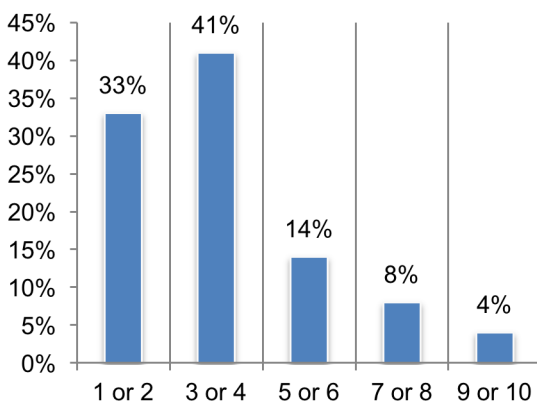
Ponemon Institute*

1. AN ACT OF CYBERWAR

The Rise of Nation State Attacks, sponsored by CounterTack and conducted by Ponemon Institute, reveals organizations' lack of readiness to respond to nation state attacks due to an uncertainty as to what a nation state attack is and how to identify the key characteristics, methods and motives of these attacks that originate with foreign governments. Without such understanding, a strategy to address the increasing likelihood of a nation state attack on an enterprise organization or a federal government agency will be difficult to achieve. Worse, the risk of

Figure 1. Rate your organization's ability to recognize a nation state attack

1 = low ability to 10 = high ability



* Sponsored by CounterTack
Independently conducted by [Ponemon Institute LLC](#)

an attack going undetected and critical organizational data exfiltrated becomes exponentially higher.

Ponemon Institute surveyed 639 U.S. IT and IT security practitioners who are familiar with their organization's ability to defend against cybersecurity attacks and have some level of responsibility in directing cybersecurity activities. Despite the experience and knowledge these respondents have, only 12 percent of respondents rate their ability to recognize a nation state attack as high (7+ on a scale of 1 = low ability to 10 = high ability), as shown in Figure 1. If nation state attacks cannot be identified and differentiated from other cyber attacks, how can enterprises know how to deal with the threats?

The urgency has skyrocketed for organizations and the federal government to become more educated in delineating between nation state threats and other cyber threats, based on the potential catastrophic impact. They also need to be better prepared and ready to react.

Following are some of the key findings from the study:

- Nearly 30 percent of respondents say a nation state attack against their organization would constitute an act of cyber war.
- Thirty-five percent of respondents say with certainty their organization has experienced a nation state attack.
- Recent nation-state attacks are worrying C-level executives. Before the Sony attack, 54 percent of senior-level executives were concerned/very

concerned about nation-state attacks. After the attacks, the response rate shot up to 74 percent being concerned, a significant shift for a singular attack.

- The attack against the U.S. government's Office of Personnel Management (OPM) shifted concern even higher for senior-level executives, up to 81 percent who are concerned/very concerned. Statistically, that's 4 out of 5 members of any given management team who are concerned now about nation-state attacks.

It's clear that nation state attacks represent a major threat against enterprise organizations in addition to government entities. However, a growing concern is how they are being perceived and dealt with. If the concern has substantially increased, why aren't companies taking action?

A. MISPERCEPTIONS ABOUT THE LIKELIHOOD OF A NATION STATE ATTACK

According to the research, there is a major misconception about how enterprises view the threat posed by nation-state attacks. Sixty-five percent of organizations represented in this study believe there is a high likelihood they will not be impacted by a nation-state attack over the next 12 months. Thus, despite recent attacks being described as having nation state actors associated with them, most organizations feel it won't happen to them.

However, looking ahead five years, 73 percent of respondents in this study say it is highly likely that they will suffer an impact from a nation-

state attack. Even more startling is that approximately half (49 percent) of respondents say their organizations are not taking precautionary measures to manage the threat. Instead they continue to procrastinate and maintain a reactive posture against threats that may have already infiltrated their systems. Furthermore, the study shows the majority of enterprises are not moving forward with a strategy to defend their organization against nation state attacks and investing in what they have identified as the most important components to help them better understand and defend against nation state attacks, which is in-house expertise and threat intelligence.

*B. CHALLENGES IN IDENTIFYING,
DEFINING AND RESPONDING TO A
NATION STATE ATTACK*

As discussed previously, participants in this study are uncertain how to identify a nation state attack. To assist in understanding, following are the characteristics of a nation state attack:

- (1) Non-state sponsored cyber attackers go after data they can sell in a short time frame such as credit card numbers and Social Security numbers.
- (2) In contrast, state sponsored attackers go after high value information that will give their countries a competitive and military advantage such as intellectual property, classified military information, schematic drawings, etc. They are motivated more by strategic than financial gain.

Of greater concern, is the difficulty organizations have in differentiating between nation

state attacks and other types of cyberattacks. The following examples are pervasive indicators that identify if a nation state is attacking an organization or a non-state sponsored attack is underway:

- Nation state attacks prey upon standard business practices and target employees in business units, who are untrained or unaware of most security practices. For example, many nation state attacks have attempted to infiltrate a network through the HR Department, using resumes submitted as attachments laced with malware.
- Depending upon the sophistication of a given enterprise's capability to detect malware and other threats that infiltrate perimeter and network protections to get to the device level, the presence of non-commodity-based malware, or purpose-built malware is a major indicator that the organization is facing a nation state threat actor who is deliberately targeting them.
- Personally Identifiable Information (PII) will always be an attractive target in terms of the data sets that attackers are after. However, Intellectual Property (IP) is arguably the most coveted information for which nation state attackers are hunting. Often industry-dependent, or geo-specific, nation state attacks seem to pursue data that will deliver competitive advantages. Indicators aren't always accurate, so it takes a new level of sophistication to be able to effectively detect and mitigate these attacks.

We conclude from the findings that despite the severity of state-sponsored attacks in 2015

against Sony, OPM and JP Morgan, many organizations seem to be taking a “wait and see” approach with their own organization. For some companies, this could prove to be a mistake. They could become the target of a breach in the not-to-distant future and will have done nothing to increase their chances of defending against the attack.

C. WE ARE NOT PREPARED

IT security practitioners, who are part of the incident response team, need to be trained to recognize and deal with nation state actors. This includes understanding the intent and indicators of a nation state attack. The following findings indicate why many participants in this study admit their organizations are not prepared to deal with nation-state attacks.

- Seventy-five percent of organizations say their organization doesn't currently have the technology or expertise to detect or prevent a nation-state attack. This points to a substantial lack of effective technology. There's a major need for more rapid and accurate detection, the ability to prevent attacks and to respond in an automated way to attacks.
- Eighty-eight percent of respondents believe nation-state attacks are hunting for network weak spots or vulnerabilities in order to establish a clear path to exfiltrate data.

D. SUMMARY

The following factors are influencing the current threat landscape:

- **Geopolitical pressure.** As evidenced by the recent United Nations Summit, there are many conversations taking place among nation states to address cyber attacks, especially against the U.S.
- **The lack of a key strategy.** Cybersecurity is shifting toward more of a real-time, data-centric discipline. Military-adopted strategies like cyber resilience focus on absorbing attacks and containing damage. Cyber resilience augments how companies and government agencies deal with attackers and should be a strategy applied to nation state attacks.
- **Media coverage.** Security trade media and journalists covering cybersecurity can be credited with pushing the cybersecurity discussion on a global scale and into the mainstream media.
- **The notion that espionage is just a “government thing.”** The Sony attack shows that there is a growing trend that nation state actors are expanding their attacks to the private sector. Just like government, companies should evaluate their attack surface regularly. They should understand the potential damage such attacks could do once inside their network or on the endpoint. Further, companies need to study where threats are originating from globally and how they might respond to attacks that are not

due to run-of-the-mill malware or low-level tactics.

In sum, many respondents say a ‘gut feel’ often dictates how to detect, define and react to nation state attacks. There is not enough information for security personnel to make critical decisions in order to defend their organizations and this is further widening their risk footprint.

2. KEY FINDINGS

In this section, we provide an analysis of the findings. The complete research findings are presented in the Appendix of this report. We have organized the report according to the following major topics:

- Enterprises believe they are vulnerable to a nation state attack
- The current response to the threat of nation state attacks: Is it enough?
- Perceptions about the motives and methods of nation state attackers
- A security strategy to protect the enterprise from nation state attacks

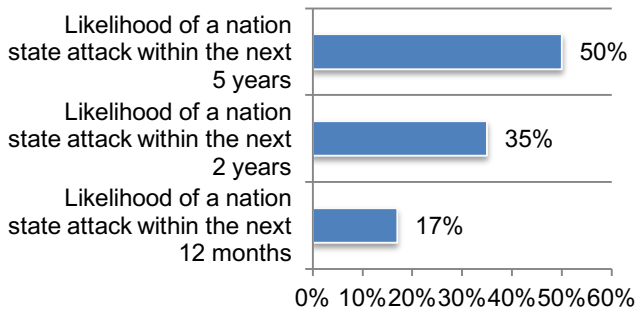
A. ORGANIZATIONS BELIEVE THEY ARE VULNERABLE TO A NATION STATE ATTACK

The likelihood of experiencing a nation state attack is increasing. Right now, only 17

percent of respondents believe a nation state attack is very likely (7+ on a scale of 1 = not likely to 10 = very likely). However, in 5 years, as shown in Figure 2, the majority of respondents believe they will experience a nation state attack.

Figure 2. Will your organization suffer a nation state attack?

Very likely 7+ on a scale from 1 = no chance to 10 = highly likely



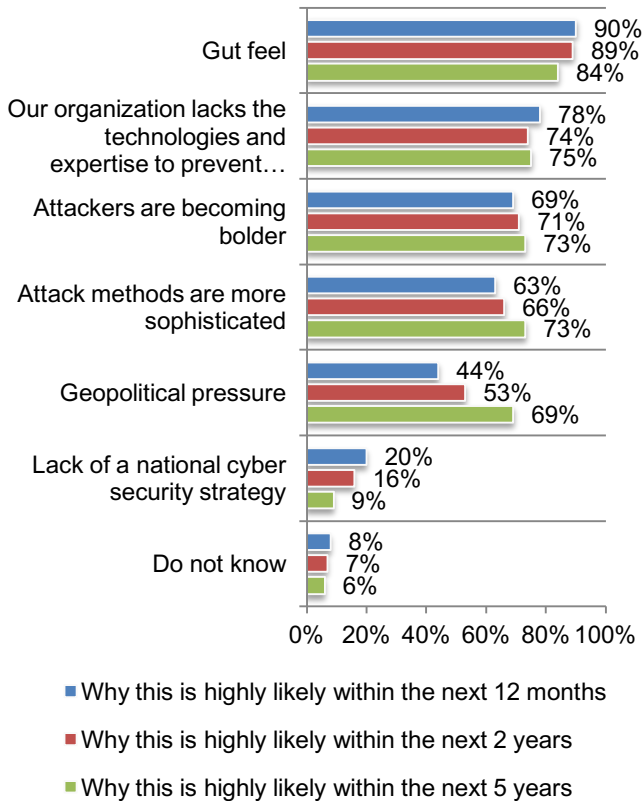
Geopolitical pressures will increase the likelihood of a nation state attack in five years.

According to Figure 3, the percentage of respondents who believe geopolitical pressures will make a nation state attack highly likely increases from 44 to 69 percent of respondents. Increasingly sophisticated attack methods are another reason nation state attacks will become more prevalent.

In general, most respondents believe nation state attacks will become more likely because of their gut feel. They also feel their organizations are vulnerable because their organizations lack the technologies and expertise to prevent such an attack.

Figure 3. Why is a nation state attack highly likely?

More than one choice permitted

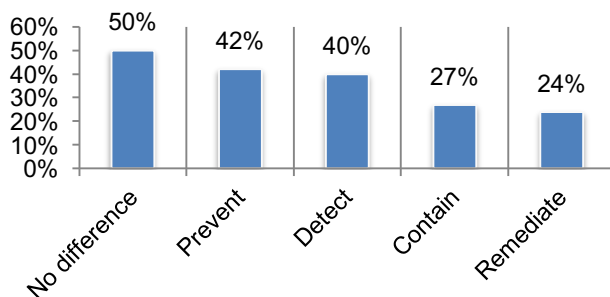


Many respondents believe nation state attacks are more difficult to prevent and detect.

As discussed previously, very few respondents are confident in their ability to identify a nation state attack. As a result, 42 percent of respondents believe

they are more difficult to prevent and 40 percent of respondents believe they are harder to detect than a cyber attack, as shown in Figure 4. Fifty percent of respondents say there is no difference between a cyber and nation state attack.

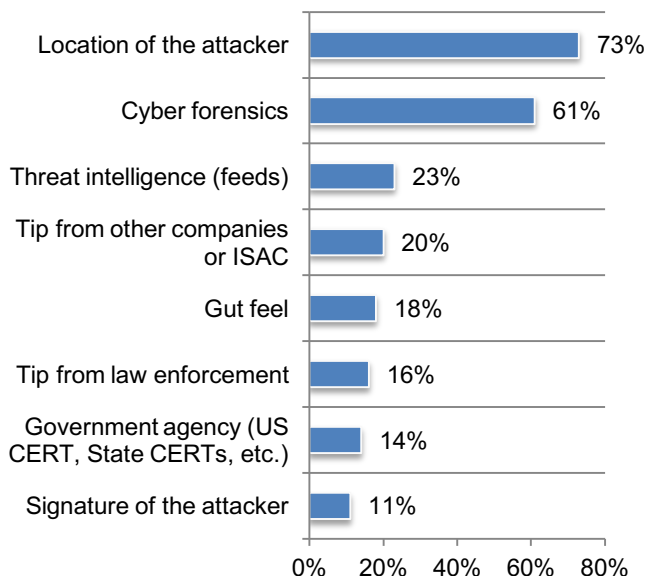
Figure 4. How do nation state attacks differ from other types of cyber attacks?



Location of the attacker is the primary indicator of a nation state attack. Twenty-one percent of organizations represented in this research say with certainty (9 percent of respondents) or that it was very likely (12 percent of respondents) their organization experienced one more nation state attacks. Sixty-five percent of respondents say their organization has not suffered a nation state attack.

According to Figure 5, those organizations that had a nation state attack say it was the location of the attacker that convinced the respondents it was such an attack (73 percent of respondents). This is followed by cyber forensics (61 percent of respondents). Rarely did the signature of the attacker (11 percent of respondents) or a government agency (14 percent of respondents) verify the incident was a nation state attack.

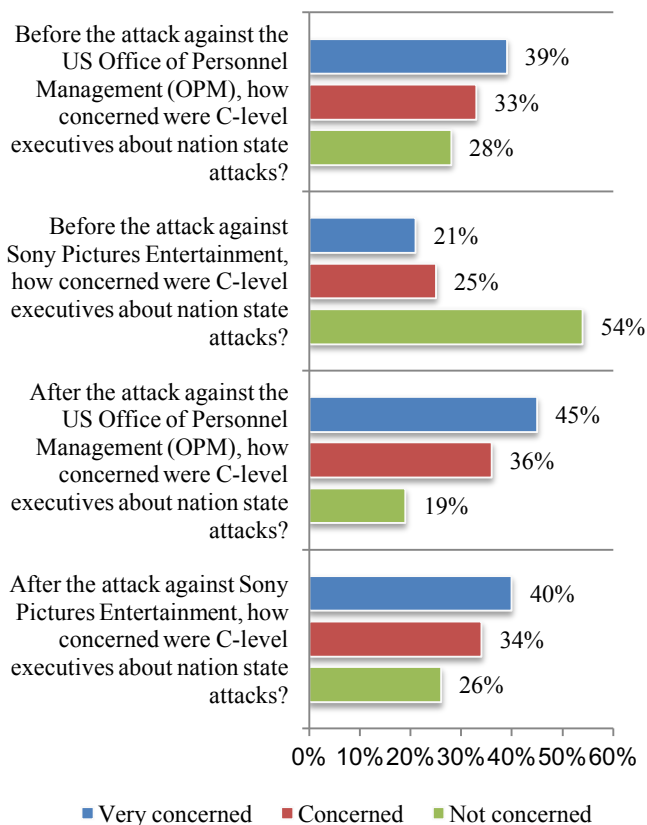
Figure 5. How did you know it was a nation state attack?



The Sony Pictures attack got the attention of senior executives. Both the attacks on Sony Pictures Entertainment and the U.S. Office of Personnel Management (OPM) increased C-level executives' worries about a possible nation state attack against their organizations, as shown in Figure 6.

Specifically, there is a very significant decrease in those respondents who say their C-level executives are not concerned about nation state attacks following the Sony attack from 54 percent of respondents to 26 percent who are not concerned. Before the attack against the OPM, 28 percent say their senior executives were not concerned and after only 19 percent were not concerned.

Figure 6. Level of concern before and after the Sony and OPM nation state attacks

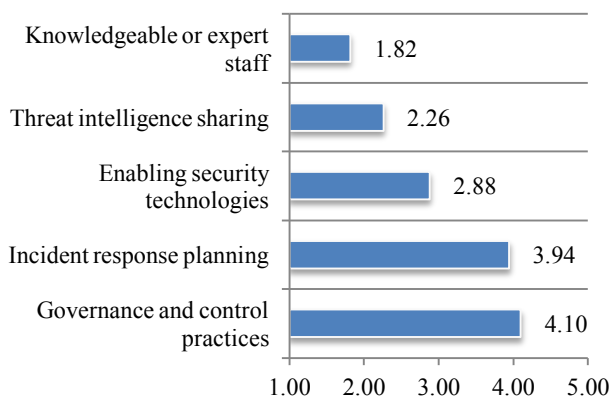


B. THE CURRENT RESPONSE TO NATION STATE ATTACKERS: IS IT ENOUGH?

Expertise and threat intelligence sharing is key to dealing with nation state attacks. While concern is growing about nation state attacks, 57 percent of respondents say their organizations are not

taking steps to improve their cyber defense against potential nation state attacks or they are unsure. However, as shown in Figure 8, respondents believe the three most important factors in protecting their organizations from a nation state attack are: knowledgeable or expert staff, threat intelligence sharing and enabling security technologies.

Figure 7. How important are the following factors in protecting your organization from a nation state attack? 1 = most important to 5 = least important



Organizations are not taking the steps they believe are important. As shown in Figure 8, less than half of respondents say their organizations are hiring experts or sharing threat intelligence. Mostly they are increasing cybersecurity budgets (62 percent of respondents), conducting training and awareness programs (59 percent of respondents) and

deploying new enabling security technologies (55 percent of respondents).

Figure 8. What changes is your organization making to defend against nation state attacks?

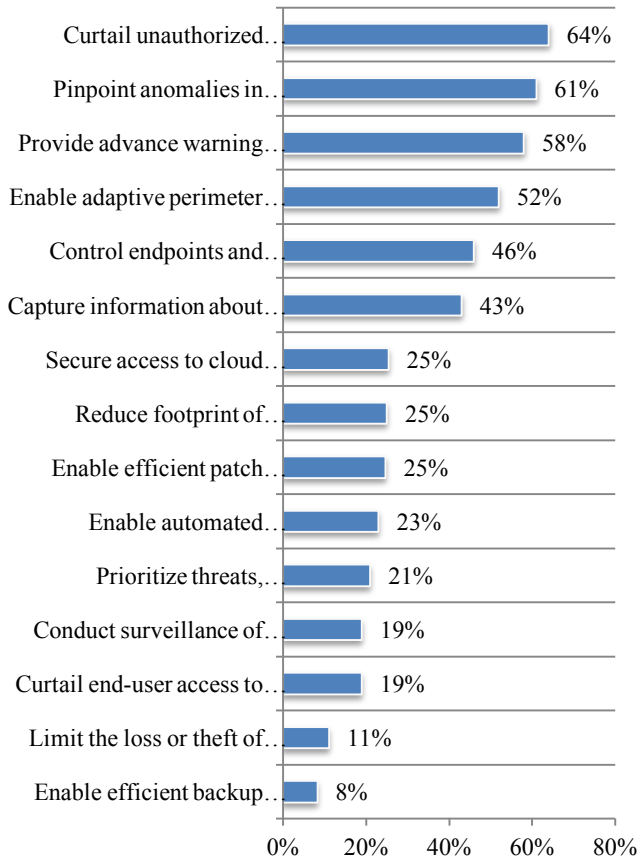


Are enterprises using the right technologies to deal with nation state attacks?

Respondents believe the following technology features are most important: the ability to curtail unauthorized access to sensitive or confidential data and mission-critical applications (64 percent of respondents), pinpoint anomalies in network traffic (61 percent of respondents), provide advance warning about threats and attackers (58 percent of respondents), enable adaptive perimeter controls (52 percent of respondents) and control endpoints and mobile connections (46 percent of respondents). However, given the nature of nation state attacks, are these the most effective?

Figure 9. The top five security technology features considered important

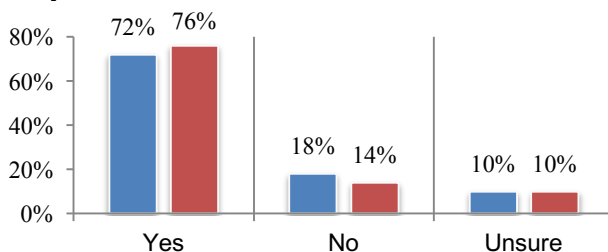
Five responses permitted



Enterprises are willing to become more aggressive in dealing with nation state attacks. According to Figure 10, 72 percent of respondents consider using offensive tools such as “hack back” or “counter hack” to stop nation states in advance of their attack on their organization and 76 percent

consider a proportional retaliation against the nation state attacker an acceptable practice.

Figure 10. Would you consider using offensive tools to stop nation states and is proportional retaliation against the nation state attacker acceptable?



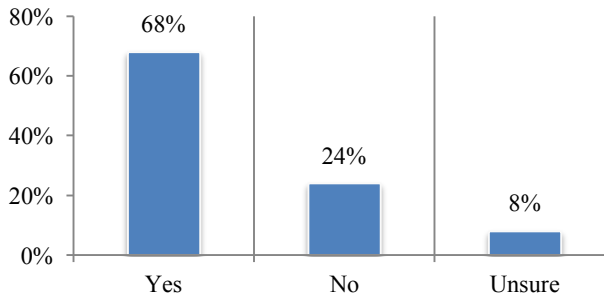
- Would your organization use offensive tools such as "hack back" or "counter hack" to stop nation states in advance of their attack
- Is proportional retaliation against the nation state attacker an acceptable practice?

Are enterprises managing the financial consequences? Because of the severe economic consequences of a cyber attack, organizations should consider the purchase of cyber liability insurance. However, only 26 percent of respondents say their organizations have such a policy and less than half (47 percent of respondents) say it covers all, or in part, the cost associated with nation state attacks.

According to Figure 11, a more popular approach to managing the risk of a nation state attack is a government-subsidized insurance policy to help the private sector reduce the financial impact of a nation state attack, according to 68 percent of respondents. However, 60 percent of respondents do not believe the government should help private

sector companies defend themselves against nation state attacks.

Figure 11. Should government-subsidized insurance help the private sector reduce the financial impact of a nation state attack?



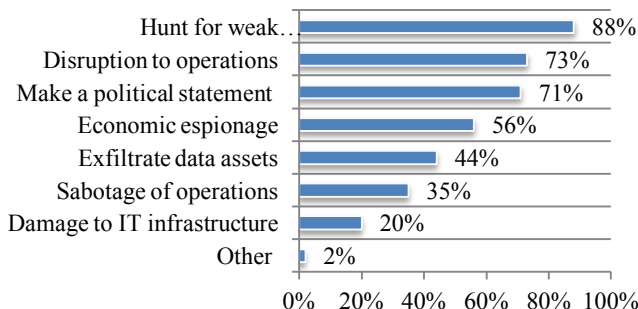
C. PERCEPTIONS ABOUT THE MOTIVES AND METHODS OF NATION STATE ATTACKERS

What are believed to be the motives of nation state attackers? According to security intelligence firm CrowdStrike's 2014 Global Threat Report, hacking has become a popular and effective weapon in geopolitical conflicts¹ The main objectives of these hackers are to hunt for weak spots/vulnerabilities, according to 88 percent of respondents, disrupt operations (73 percent of respondents) and to make a political statement (71 percent of respondents).

Figure 12. What are the main objectives of nation state attackers?

¹ Kelly Jackson Higgins, *Nation-State Cyber Espionage, Targeted Attacks Becoming Global Norm*, Dark Reading February 10, 2015.

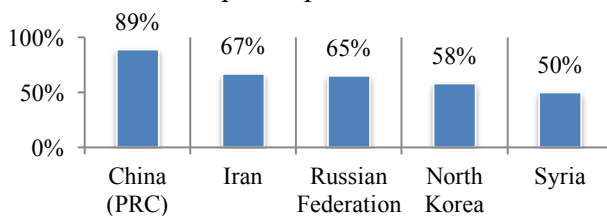
More than one response permitted



The countries believed to support or facilitate most potential state attacks against their organizations are shown in Figure 13. By far, China is viewed as the biggest threat. The CrowdStrike report names China as “the number one active and most prolific nation waging cyber espionage attacks”. However, “threat groups with ties to Russia and Iran—and North Korea—expanded their targeted attack campaigns in the past year”.²

Figure 13. Which countries do you think would support or facilitate most potential nation state attacks against their organization?

More than one response permitted

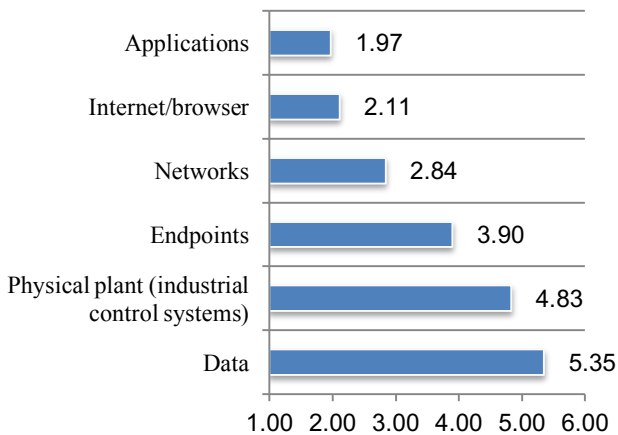


What are the methods of nation state attackers? How are nation state attacks most likely to infiltrate an organization’s systems? According to

² Ibid (February 10, 2015).

Figure 14, most likely the attack is made through applications followed by the Internet/browser and networks.

Figure 14. Where are nation state attacks most likely to infiltrate your organization’s systems?
1 = most likely to 6 = least likely



D. A SECURITY STRATEGY TO PROTECT THE ENTERPRISE FROM NATION STATE ATTACKS

Today’s dynamic threat landscape means that organizations must deal not only with individual cyber attackers but foreign governments determined to steal information for political, military and competitive purposes. Some recommendations from security experts include the following:³

- Do not acquire technology from companies based in nations that pose a threat, such as China and Russia.

³ Eric Chabrow, *4 Ways to Defend against Nation-State Attacks*, GovinfoSecurity, May 10, 2013.

- The safest way to protect data from nation state attackers is to remove internal systems from the Internet entirely. Access to the Internet should be physically isolated from the internal network with one-way, tightly secured paths to move data into and out of the internal network, according to Robert Bigman, former CISO at the U.S. Central Intelligence Agency.
- Intelligence sharing is important to protect against nation state attacks. Sharing of cyber threat information among businesses and government could help reduce attacks. In this study, 66 percent of respondents believe there should be a cross-industry and government initiative to help organizations build a strong defense against nation state attackers.
- Regularly train and test employees' understanding of such security threats as phishing and spear-phishing.

3. METHODS

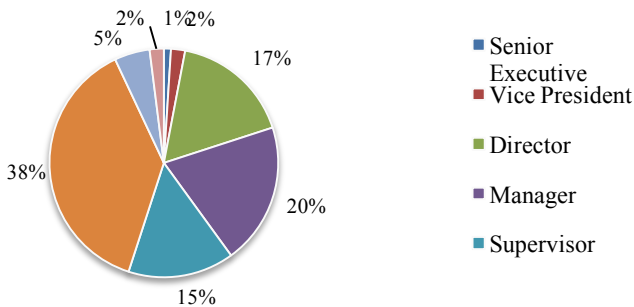
A random sampling frame of 17,475 IT and IT security practitioners located in all regions of the United States were selected as participants to this survey. As shown in Table 1, 713 respondents completed the survey. Screening removed 74 surveys. The final sample was 639 surveys (or a 3.7 percent response rate).

Table 1. Sample response	Freq.	Pct%

Total sampling frame	17,475	100.0%
Total returns	713	4.1%
Rejected or screened surveys	74	0.4%
Final sample	639	3.7%

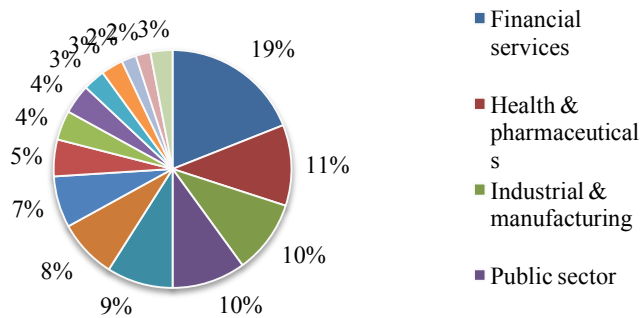
Pie Chart 1 reports the respondents' current position. More than half of respondents (55 percent) are at or above the supervisory level.

Pie Chart 1. Respondent's current position



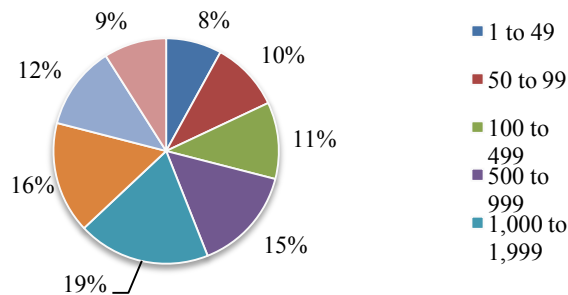
Pie Chart 2 reports the respondents' primary industry segments. Nineteen percent of respondents are in financial services and 11 percent are in health and pharmaceuticals. Another 10 percent are in industrial & manufacturing and public sector.

Pie Chart 2. Distribution of respondents according to primary industry classification

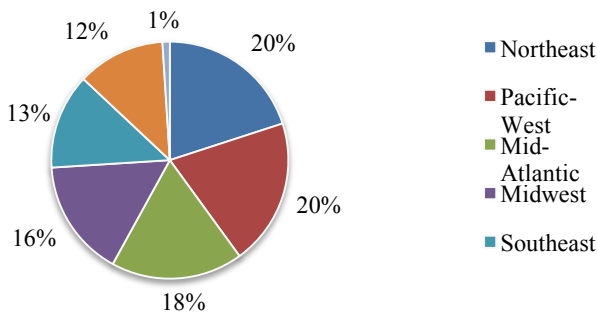


Fifty-six percent of respondents are from organizations with a global headcount greater than 1,000 as shown in Pie Chart 3.

Pie Chart 3. Worldwide headcount



Pie Chart 4 reveals the regional location of the respondents. Twenty percent of respondents are in the Northeast with another twenty percent in the Pacific-West and 18 percent are located in the Mid-Atlantic region.

Pie Chart 4. Regional location

4. CAVEATS

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners. 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 February 2015.

Survey response	Freq	Pct%
Total sampling frame	17475	100.0%
Total returns	713	4.1%
Rejected or screened surveys	74	0.4%
Final sample	639	3.7%

Part 1. Screening

S1. How familiar are you with your organization's ability to defend against cyber security attacks?	Pct%
Very familiar	54%
Familiar	33%
Somewhat familiar	13%
No knowledge (Stop)	0%
Total	100%

S2. Do you have any responsibility in directing cyber security activities within your organization?	Pct%
Yes, full responsibility	32%
Yes, some responsibility	39%
Yes, minimum responsibility	29%
No responsibility (Stop)	0%

Total	100%
-------	------

Part 2. Questions

Q1. Using the following 10-point scale, please rate your organization's ability to recognize a nation state attack from 1 = low to 10 = high.	Pct%
1 or 2	33%
3 or 4	41%
5 or 6	14%
7 or 8	8%
9 or 10	4%
Total	100%
Extrapolated value	3.68

Q2a. Using the following 10-point scale, please rate the likelihood that your organization will suffer a nation state attack from 1 = no chance to 10 = very likely within the next 12 months.	Pct%
1 or 2	41%
3 or 4	23%
5 or 6	19%
7 or 8	15%
9 or 10	2%
Total	100%
Extrapolated value	3.78

Q2b. If you believe this is highly likely (a rating 7 and higher), why? Please select all that apply.	Pct%
Attackers are becoming bolder	69%
Attack methods are more sophisticated	63%
Geopolitical pressure	44%
Lack of a national cyber security strategy	20%
Our organization lacks the technologies and expertise to prevent such an attack	78%
Gut feel	90%
Do not know	8%
Total	372%

Q3a. Using the following 10-point scale, please rate the likelihood that your organization will suffer a nation state attack from 1 = no chance to 10 = very likely within the next 2 years.	Pct%
1 or 2	21%
3 or 4	21%
5 or 6	23%
7 or 8	19%
9 or 10	16%
Total	100%
Extrapolated value	5.26

Q3b. If you believe this is highly likely (a rating 7 and higher), why? Please select all that apply.	Pct%
Attackers are becoming bolder	71%
Attack methods are more sophisticated	66%
Geopolitical pressure	53%
Lack of a national cyber security strategy	16%
Our organization lacks the technologies and expertise to prevent such an attack	74%
Gut feel	89%
Do not know	7%
Total	376%

Q4a. Using the following 10-point scale, please rate the likelihood that your organization will suffer a nation state attack from 1 = no chance to 10 = very likely within the next 5 years.	Pct%
1 or 2	12%
3 or 4	15%
5 or 6	23%
7 or 8	27%
9 or 10	23%
Total	100%
Extrapolated value	6.18

Q4b. If you believe this is highly likely (a rating 7 and higher), why? Please select all that apply.	Pct%
Attackers are becoming bolder	73%
Attack methods are more sophisticated	73%
Geopolitical pressure	69%
Lack of a national cyber security strategy	9%
Our organization lacks the technologies and expertise to prevent such an attack	75%
Gut feel	84%
Do not know	6%
Total	389%

Q5a. Has your organization experienced one or more nation state attacks?	Pct%
Yes, with certainty'	9%
Yes, very likely	12%
Yes, likely	14%
No	65%
Total	100%

Q5b. If yes, how did you know this was a nation state attack? Please select all that apply.	Pct%
Cyber forensics	61%
Threat intelligence (feeds)	23%
Location of the attacker	73%
Signature of the attacker	11%

Tip from law enforcement	16%
Tip from other companies or ISAC	20%
Government agency (US CERT, State CERTs, etc.)	14%
Gut feel	18%
Other (please specify)	0%
Total	236%

Q6a. Before the cyber attack against Sony Pictures Entertainment, how concerned were your organization's C-level executives about nation state attacks?	Pct%
Very concerned	21%
Concerned	25%
Not concerned	54%
Total	100%

Q6b. After the cyber attack against Sony Pictures Entertainment, how concerned were your organization's C-level executives about nation state attacks?	Pct%
Very concerned	40%
Concerned	34%
Not concerned	26%
Total	100%

Q6c. Before the cyber attack against the US	Pct%
---	------

Office of Personnel Management (OPM), how concerned were your organization's C-level executives about nation state attacks?	
Very concerned	39%
Concerned	33%
Not concerned	28%
Total	100%

Q6d. After the cyber attack against the US Office of Personnel Management (OPM), how concerned were your organization's C-level executives about nation state attacks?	Pct%
Very concerned	45%
Concerned	36%
Not concerned	19%
Total	100%

Q7a. Is your organization taking steps to improve its cyber defense against potential nation state attacks?	Pct%
Yes	43%
No	49%
Unsure	8%
Total	100%

Q7b. If yes, what changes are being made	Pct%
--	------

by your organization? Please select all that apply	
Increasing cyber security budget	62%
Deploying new enabling security technologies	55%
Hiring expert or knowledgeable staff	48%
Revising incident response procedures	45%
Implementing threat sharing with other organizations	38%
Establishing link with law enforcement and government	11%
Implementing governance and control procedures	50%
Conducting training and awareness programs	59%
Conducting risk assessments	50%
Other (please specify)	3%
Total	421%

Q8. In your opinion, how do nation state attacks differ from other types of cyber attacks? Please select all that apply. Nation state attacks are harder to . . .	Pct%
Detect	40%

Prevent	42%
Contain	27%
Remediate	24%
No difference	50%
Total	183%

Q9. In your opinion, how important are the following factors in protecting your organization from nation state attackers? Please rank the following list from 1 = most important to 5 = least important.	Average rank	Rank order
Knowledgeable or expert staff	1.82	1
Enabling security technologies	2.88	3
Threat intelligence sharing	2.26	2
Governance and control practices	4.10	5
Incident response planning	3.94	4
Total	3.00	

Q10. What do you think are the main objectives of nation state attackers? Please select all that apply.	Pct%
Economic espionage	56%
Sabotage of operations	35%
Disruption to operations	73%

Damage to IT infrastructure	20%
Hunt for weak spots/vulnerabilities	88%
Make a political statement	71%
Exfiltrate data assets	44%
Other (please specify)	2%
Total	389%

Q11. Where are nation state attacks most likely to infiltrate your organization's systems? Please rank the following 6 system entry points from 1 = most likely to 6 = least likely.	Average rank	Rank order
Endpoints	3.90	4
Networks	2.84	3
Internet/browser	2.11	2
Applications	1.97	1
Data	5.35	6
Physical plant (industrial control systems)	4.83	5
Total	3.50	

Q12. In your opinion, should the government help private sector companies defend themselves against nation state attacks?	Pct%
Yes	34%
No	60%

Unsure	6%
Total	100%

Q13. In your opinion, would a nation state attack against your company or industry constitute an act of cyber war?	Pct%
Yes	29%
No	36%
Unsure	35%
Total	100%

Q14a. Does your organization have cyber liability insurance?	Pct%
Yes	26%
No	56%
Unsure	18%
Total	100%

Q14b. If yes, does the policy cover all, or in part, the cost associated with nation state attacks?	Pct%
Yes	47%
No	42%
Unsure	11%
Total	100%

Q15. In your opinion, should there be government-subsidized insurance to help the	Pct%
---	------

private sector reduce the financial impact of a nation state attack?	
Yes	68%
No	24%
Unsure	8%
Total	100%

Q16. In your opinion, would you consider using offensive tools such as “hack back” or “counter hack” to stop nation states in advance of their attack on your organization?	Pct%
Yes	72%
No	18%
Unsure	10%
Total	100%

Q17. In your opinion, is proportional retaliation against the nation state attacker an acceptable practice?	Pct%
Yes	76%
No	14%
Unsure	10%
Total	100%

Q18. In your opinion, should there be a cross-industry/government initiative to help	Pct%
--	------

organizations build a strong defense against nation state attackers?	
Yes	66%
No	30%
Unsure	4%
Total	100%

Q19. Which countries do you think would support or facilitate most potential nation state attacks against your organization? Please select your top five countries from the followi[Insert country pull down list]	Pct%
China (PRC)	89%
Iran	67%
Russian Federation	65%
North Korea	58%
Syria	50%

Q20. Following are 15 cyber security technology features considered important by many organizations. Please select 5 technology features that you consider most important in defending your	Pct%
---	------

organization from nation state attackers.	
Curtail unauthorized access to sensitive or confidential data and mission-critical applications	64%
Pinpoint anomalies in network traffic	61%
Provide advance warning about threats and attackers	58%
Enable adaptive perimeter controls	52%
Control endpoints and mobile connections	46%
Capture information about attackers (honey pot)	43%
Secure access to cloud resources	25%
Reduce footprint of sensitive or confidential data	25%
Enable efficient patch management	25%
Enable automated remediation	23%
Prioritize threats, vulnerabilities and attacks	21%
Curtail end-user access to insecure Internet sites and web applications	19%
Conduct surveillance of system users	19%

Limit the loss or theft of portable data-bearing devices	11%
Enable efficient backup and disaster recovery operations	8%
Total	500%

Part 3. Organization characteristics and respondent demographics

D1. What organizational level best describes your current position?	Pct%
Senior Executive	1%
Vice President	2%
Director	17%
Manager	20%
Supervisor	15%
Technician	38%
Staff or Administrative	5%
Contractor	1%
Other (please specify)	1%
Total	100%

D2. US regional location	Pct%
Northeast	20%
Mid-Atlantic	18%
Midwest	16%
Southeast	13%
Southwest	12%
Pacific-West	20%

Other (please specify)	1%
Total	100%

D3. What industry best describes your organization's industry concentration or focus?	Pct%
Agriculture & food services	1%
Communications	2%
Consumer products	5%
Defense & aerospace	1%
Education & research	2%
Energy & utilities	4%
Entertainment & media	3%
Financial services	19%
Health & pharmaceuticals	11%
Hospitality	4%
Industrial & manufacturing	10%
Public sector	10%
Retail	9%
Services	8%
Technology & software	7%
Transportation	3%
Other (please specify)	1%
Total	100%

D4. What is the worldwide headcount of your organization?	Pct%
---	------

1 to 49	8%
50 to 99	10%
100 to 499	11%
500 to 999	15%
1,000 to 1,999	19%
2,000 to 4,999	16%
5,000 to 9,999	12%
10,000 or more	9%