Ponemon INSTITUTE

State of IT Security

Study of Utilities & Energy Companies

Sponsored by Q1 Labs

Independently conducted by Ponemon Institute LLC

Publication Date: April 2011

State of IT Security: Study of Utilities & Energy Companies

Ponemon Institute, April 2011

Part 1. Executive summary

Ponemon Institute is pleased to present the results of *State of IT Security: Study of Utilities & Energy Companies*. Sponsored by Q1 Labs, the purpose of this research is to better understand how organizations determine their state of readiness to a plethora of information security and data protection risks – including those emerging from SCADA networks and smart grid communications. The study also focuses on the people, process and technologies deployed by utilities and energy companies to maintain a high level of vigilance.

A total of 291 IT and IT security practitioners in utilities and energy companies with an average of 11 years of experience participated in this study. The work of participants in our study involves securing the organization's information assets, enterprise systems or critical infrastructure. They also have some level of familiarity with NERC CIP and other related standards on the protection of cyber assets and the critical infrastructure. Topics covered in this research include:

- Do global energy organizations view IT security as a strategic initiative across the enterprise?
- Is compliance with industry-related regulatory initiatives a priority?
- How frequent do these organization experience data breaches?
- Are existing controls designed to protect against exploits and attacks through smart grid and smart meter-connected systems?

We believe this study is important because cyber attacks on critical infrastructure companies may be on the rise. According to a new study by the Center for Strategic and International Studies (CSIS) there has been a jump in extortion attempts and malware designed to sabotage systems, like Stuxnet.[1] The report is consistent with our study that many companies are not doing enough to protect their systems and are rushing to adopt new technologies (such as smart grid) without the appropriate security technologies or controls in place.

In fact, our study reveals that only 9 percent of respondents believe their organization's security initiative is very effective in providing actionable intelligence (such as real-time alerts, threat analysis and prioritization) about potential and actual exploits on their systems. Fifty percent of respondents report that they do not receive this intelligence at all. Further, 61 percent have not deployed SIEM although 73 percent say it benefits companies by bridging gaps among departments such as IT operations, network operations, data center management and others.

Recommendations to help companies understand what steps they need to do to protect their systems are available. In September 2010, The National Institute of Standards and Technology (NIST) issued its first *Guidelines for Smart Grid Cyber Security (NISTIR 7628)*, which includes high-level security requirements, a framework for assessing risks, an evaluation of privacy issues at personal residences, and additional information for businesses and organizations to use as they craft strategies to protect the modernizing power grid from attacks, malicious code, cascading errors, and other threats. NIST recommends 189 high-level security requirements applicable either to the entire Smart Grid or to particular parts of the grid and associated interface categories.[2]

The key findings of this research are presented in the next section. It is followed by a description of our survey methods and our summarized concluding thoughts. The appendix to this paper presents the frequencies or percentage frequencies to all survey questions. We also provide the sample size to each question posed to respondents.

---

[1] Cyber attacks rise at critical infrastructure firms, by Elinor Mills, CNET.com, April 18, 2011

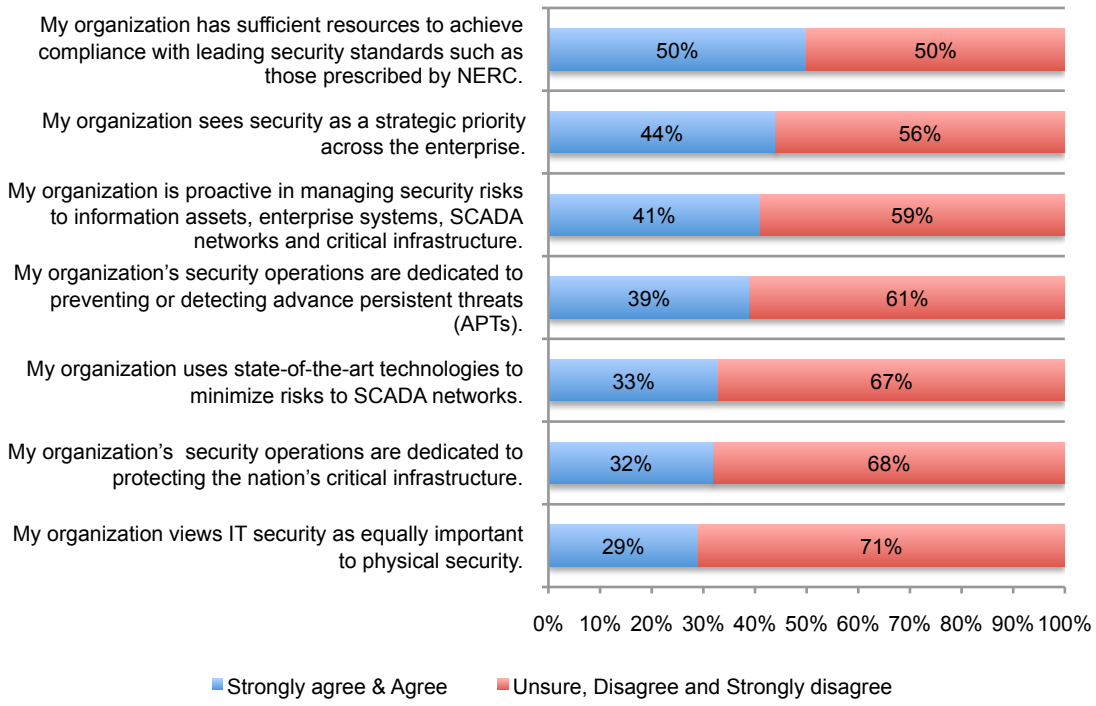
[2] See "NIST Finalizes Initial Set of Smart Grid Cyber Security Guidelines," press release, September 2, 2010

Part 2. Key findings

A majority of respondents in this study say their organizations do not view IT security as a strategic imperative for the enterprise.

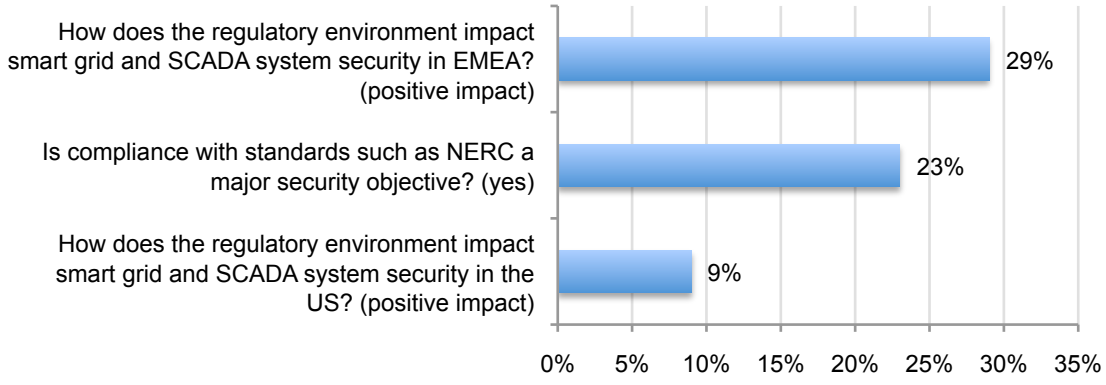
According to 71 percent of respondents, the management team in their organizations does not understand or appreciate the value of IT security. As a consequence of this perception among C-level executives, only 39 percent of energy organizations say their security program is dedicated to detecting or preventing Advanced Persistent Threats and 67 percent are **not** using what would be considered "state of the art" technologies to minimize risks to SCADA networks. Forty-one percent do not view their security operations as proactive in managing risks associated with SCADA networks and critical infrastructure.

Bar Chart 1: Attributions about the state of IT security



Only a small percentage of respondents say compliance with regulatory requirements such as NERC CIP is a major security initiative within their organizations.

Bar Chart 2: Perceptions about compliance with industry-related regulations

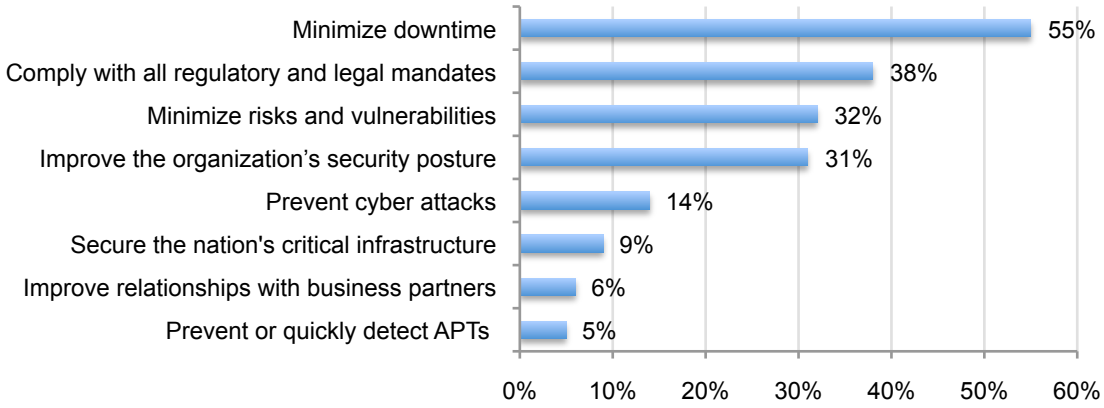


While most respondents see the protection of SCADA systems as a priority, only 9 percent say compliance requirements positively impact the security posture for companies located in the U.S. In contrast, 29 percent of respondents say compliance requirements in EMEA positively impact their companies' security posture.

System downtime and not the threat of a cyber attack is the most important goal of the security program. This priority most likely influences how resources for security investments are allocated. Only 14 percent of respondents say prevention of cyber attacks is a priority, 5 percent say detecting advanced persistent threats (APT) is important, and 9 percent say it should be securing systems connected to the smart grid.

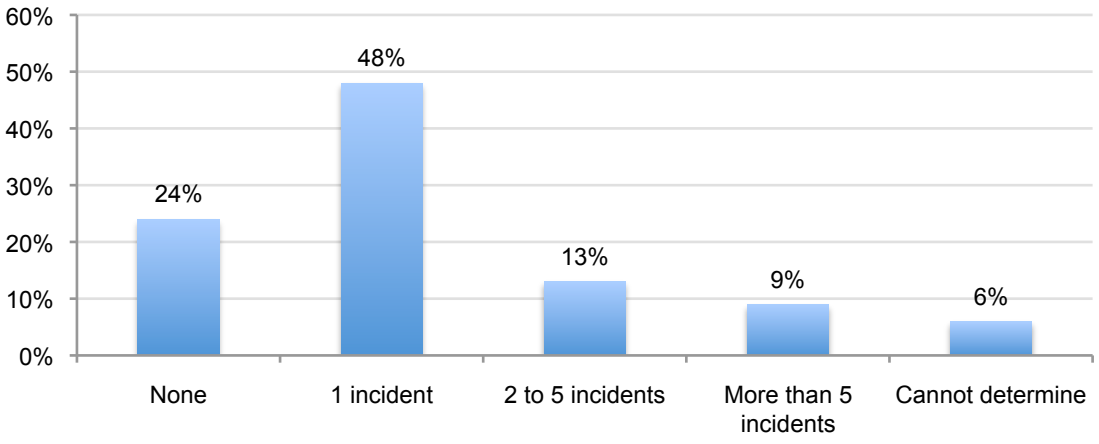
Bar Chart 3 shows the second most important security objective (38 percent) concerns achieving compliance with all regulatory and legal mandates. In light of the results in Bar Chart 2, there appears to be a disconnection between actual practice and the stated objectives of the IT security function. Such gaps suggest these organizations are at risk for non-compliance with regulations and are more vulnerable to attacks.

Bar Chart 3: Top IT security objectives or mission
More than one response is permitted



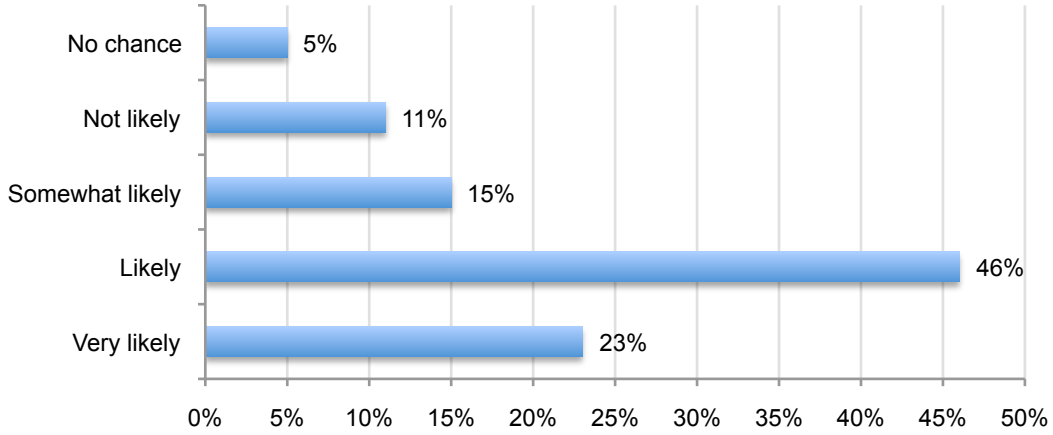
According to Bar Chart 4, 76 percent of respondents' organizations have suffered one or more data breaches during the past 12 months. Twenty-two percent say their organizations have experienced two or more data breach incidents.

Bar Chart 4: Frequency of data breaches
Only one response required



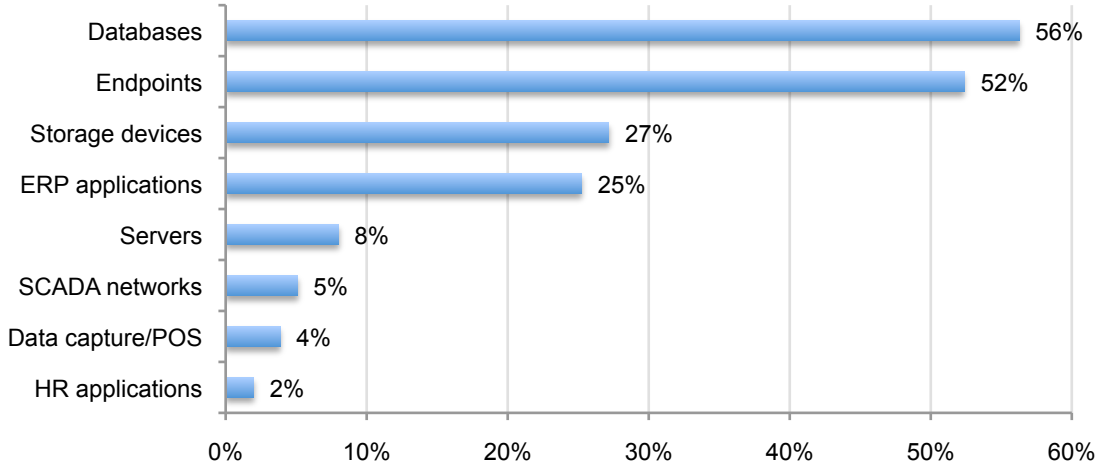
Bar Chart 5 shows 69 percent say they believe a successful exploit on their organization's network is very likely (23 percent) or likely (46 percent) to occur over the next 12 months.

Bar Chart 5: The likelihood of a successful exploit
Only one response required



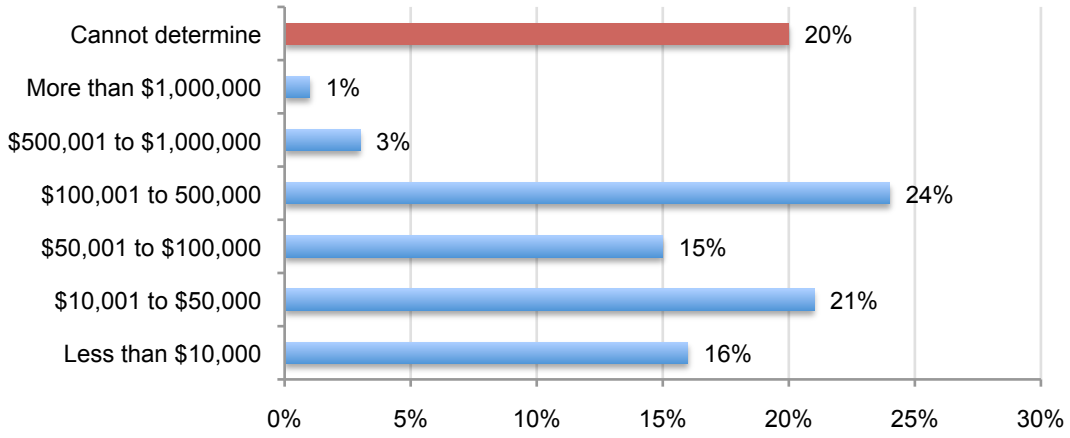
Bar Chart 6 shows that 56 percent of respondents say databases and 52 percent say endpoints were the two top core systems compromised as a result of IT security incidents during the past 12 months. Only 5 percent of respondents say SCADA networks were compromised as a result of IT security incidents.

Bar Chart 6: Core systems compromised as a result of IT security incidents
More than one response is permitted



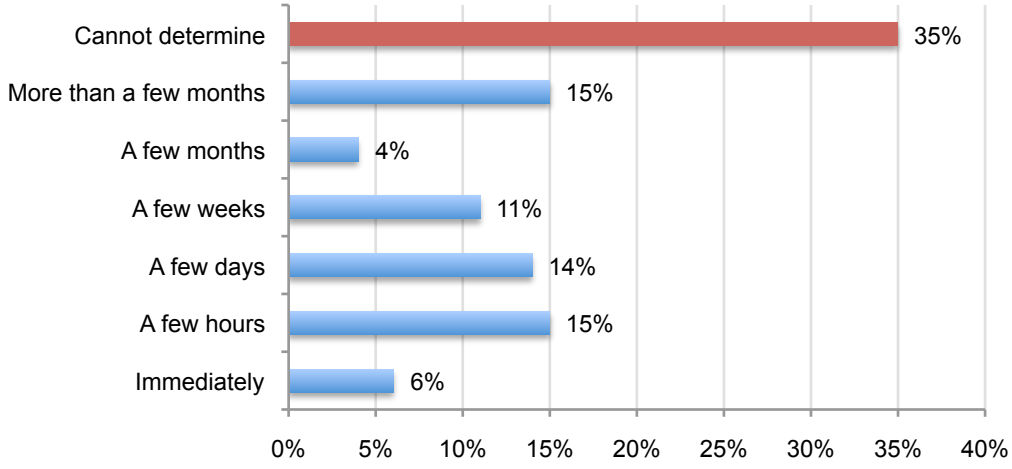
The extrapolated average cost of IT security incidents experienced by respondents' organizations is $156,000. As shown in Bar Chart 7, about 20 percent of respondents could not estimate a value. Only 4 percent see the average cost as more than $500,000.

Bar Chart 7: Extrapolated average cost incurred as a result of IT security incidents experienced over the past 12 months
Only one response required



On average, it takes 22 days to detect an insider who made some type of unauthorized change or committed some sort of malicious activity. Bar Chart 8 shows 35 percent of respondents could not estimate a time value. Only 6 percent believe detection would happen immediately or in less than one hour.

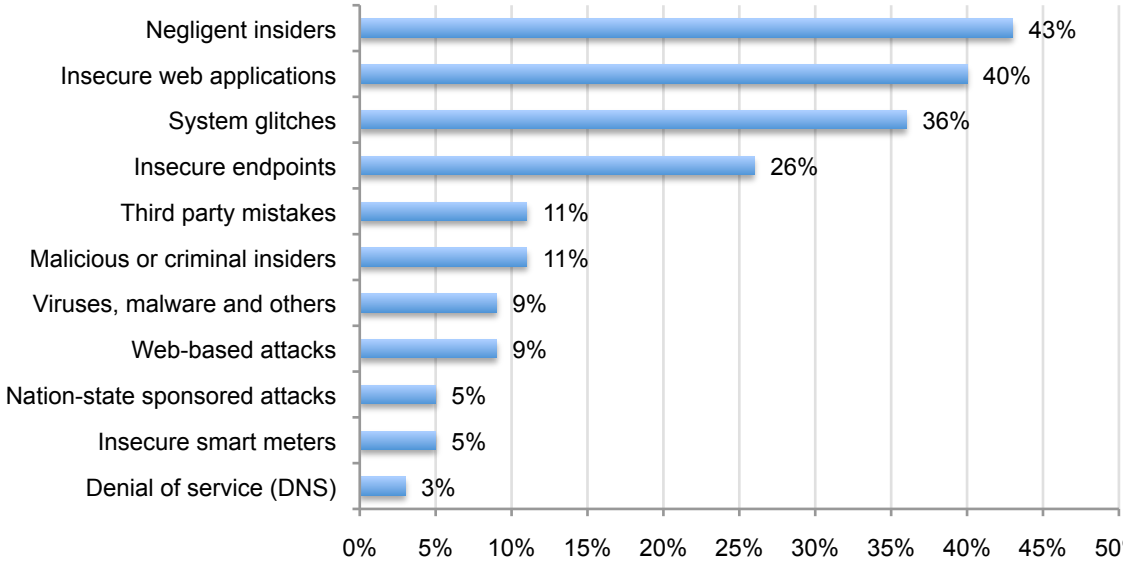
Bar Chart 8: Approximate length of time to detect an insider who made some type of unauthorized change or committed some sort of malicious activity
Only one response required



Insider negligence is a problem for these organizations.

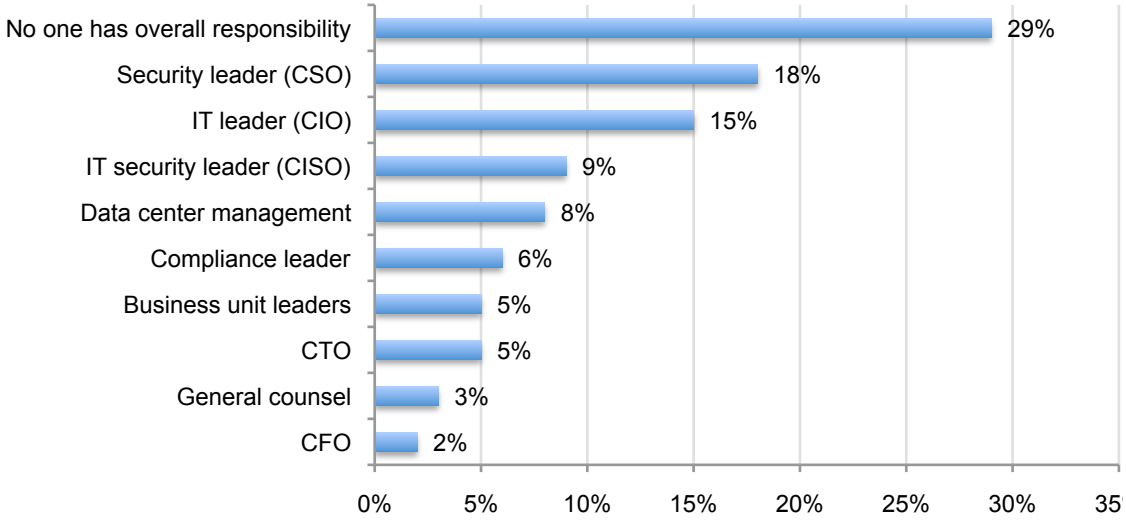
Bar Chart 9 lists the top IT security threats experienced by respondents. According to 43 percent of respondents, the top-ranked security threat their organizations faces is negligent insiders. Insecure web applications and system glitches are also significant security threats (40 percent and 36 percent, respectively).

Bar Chart 9: The top IT security threats that affect respondents' organizations
More than one response is permitted



A lack of leadership and overall accountability for security program management could be contributing to security risks. Bar Chart 10 reports the functional leaders who have ultimate responsibility for security. In 29 percent of the organizations in this study, no one role has overall responsibility. Eighteen percent say the security leader has overall responsibility for the management of the organization's security objectives.

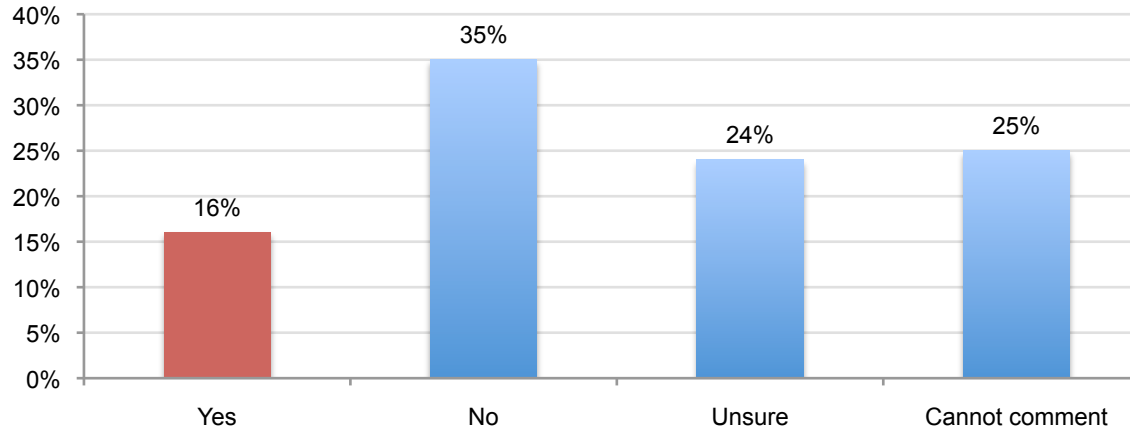
Bar Chart 10: Who is most responsible for ensuring security objectives are achieved?
Only one response required



Although IT and IT security practitioners worry about the security of the smart grid, few believe existing controls are sufficient to stop attacks and exploits.

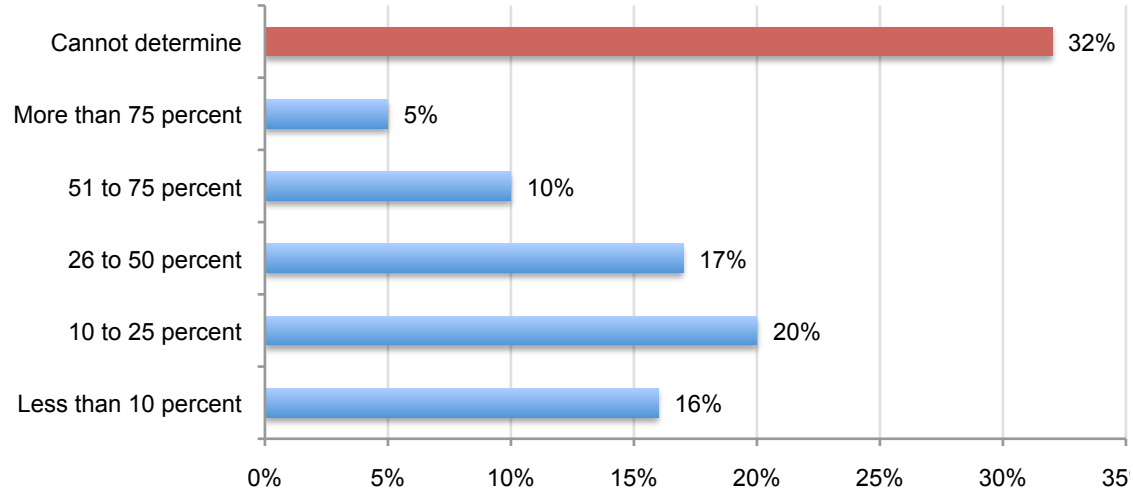
As noted in Bar Chart 11, only 16 percent of respondents believe the existing controls in their organizations are designed to specifically protect against exploits and attacks through smart grid and smart meter-connected systems.

Bar Chart 11: Do you feel your organization's existing security controls provide adequate levels of protection against attacks and exploits occurring through smart meters and smart grid systems?
Only one response required



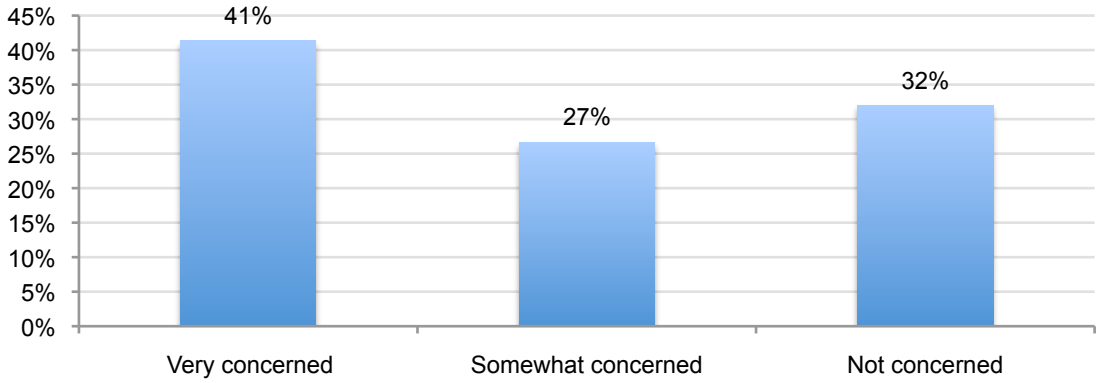
Additionally, about 30 percent of respondents believe the overall network telemetry is out of their direct control. Bar Chart 12 shows that 15 percent of respondents say that more than half of their organizations' network components are outside their direct control.

Bar Chart 12: Percent of network components, including third-party endpoints such as smart phones and home computers, outside the direct control of security operations
Only one response required



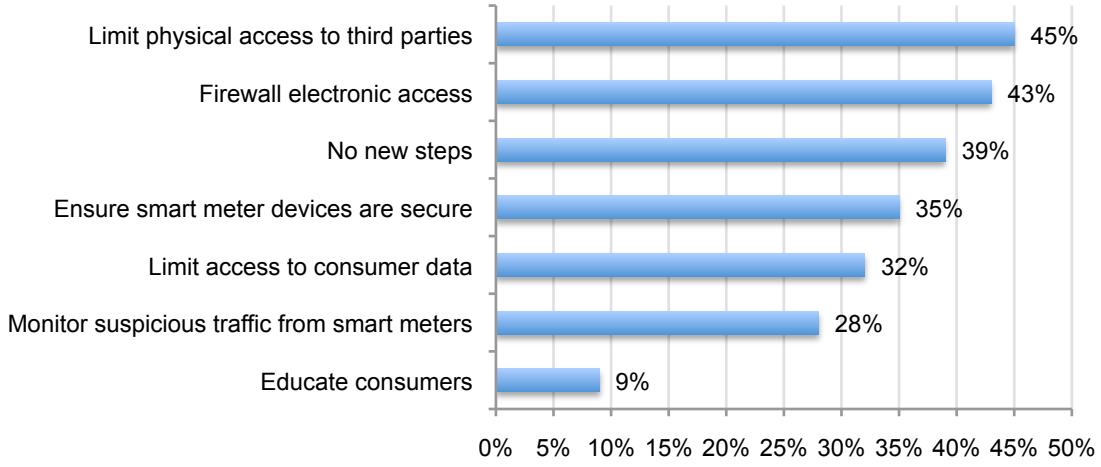
Sixty-eight percent of respondents are somewhat (27 percent) or very concerned (41 percent) about the risks posed by third party providers that are connected to the smart grid.

Bar Chart 13: Respondents' level of concern about third-party providers who are (or will be) connected to the smart grid
Only one response required



Bar Chart 14 shows 45 percent of respondents say their organizations are focused on limiting physical access to third parties involved with the smart grid. Forty-three percent say smart grid security is achieved through improved perimeter controls such as firewalls. Thirty-nine percent say their organizations have not implemented any new steps to secure smart grid communications. Only 28 percent of respondents' organizations say they monitor suspicious traffic originating from smart meters.

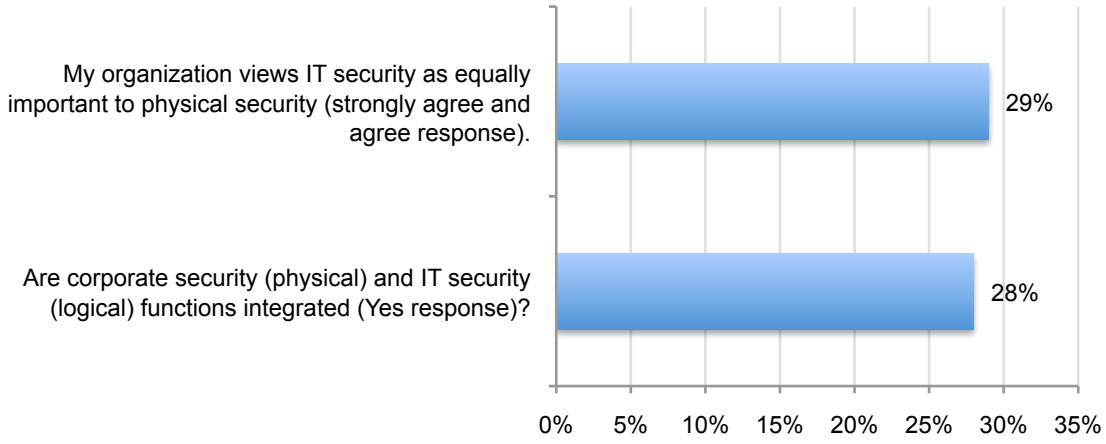
Bar Chart 14: New steps taken to secure the smart grid
More than one response is permitted



Respondents believe their organizations' security mission is primarily focused on physical security rather than IT security.

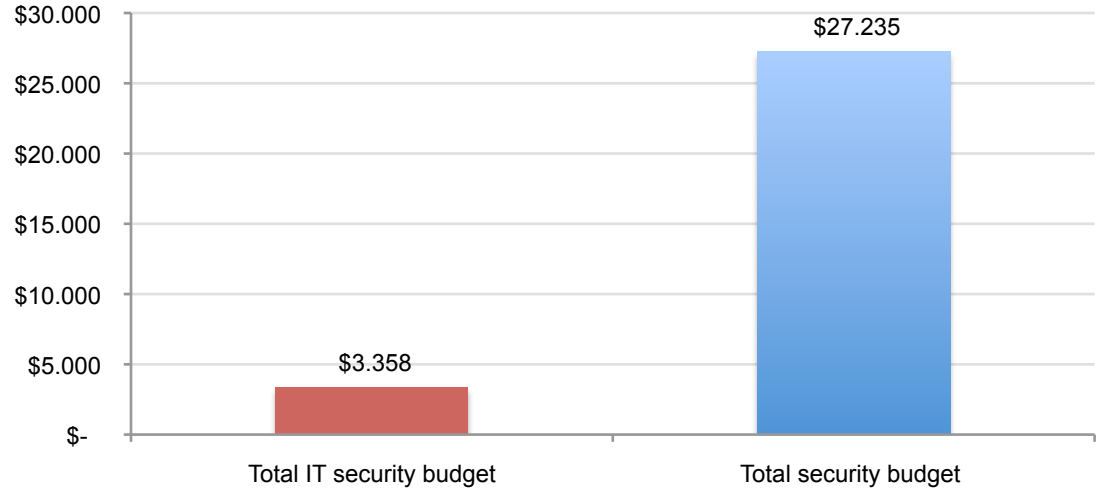
Bar Chart 15 provides clear evidence that respondents' organizations focused on the protection of property, plant and other physical assets rather than electronic records or enterprise systems. Accordingly, only 29 percent believe the organization views IT and physical security as equals in terms of a priority.

Bar Chart 15: Is physical security more important than IT security among respondents' organizations?
These are two separate survey questions



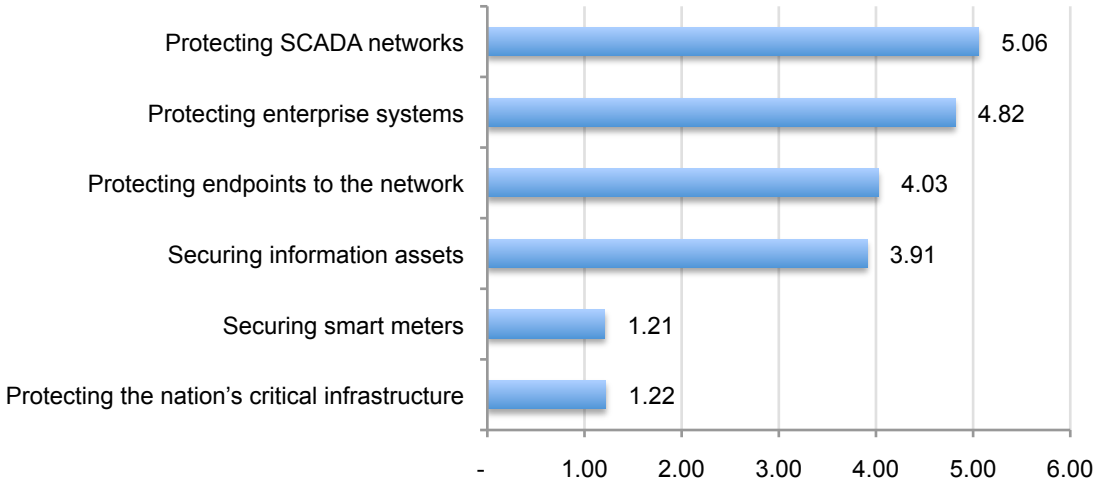
Bar Chart 16 reports extrapolated average results on the budgeted amounts or earmarks for IT and physical security. As can be seen, organizations are spending considerably fewer dollars on IT security than physical security. This results further supports the proposition that respondents' organizations do not see IT security as a primary area of focus.

Bar Chart 16: Extrapolated average cost of IT and physical security budgets in the present fiscal year
1,000,000 omitted



The following chart lists in descending order the average rank assigned to six IT security priorities. The top two priorities include protecting SCADA networks and enterprise systems. The bottom two priorities including protecting the nation's critical infrastructure or security smart meters.

Bar Chart 17: Average rank order the following six security priorities from 6 = highest priority to 1 = lowest priority (for the series).



Part 3. Methods

Table 1 summarizes the sample response for this study. Our sampling frame of practitioners consisted of 8,220 individuals located in the United States who have bona fide credentials in the IT or IT security fields. This resulted in 384 individuals completing the survey of which 46 were rejected for reliability issues. Our final sample before screening was 338. Another 47 individuals were removed because of sample screening procedures, thus resulting in a final sample of 291 respondents (3.5 percent response rate).

Table 1: Sample response	Freq.
Sampling frame	8,220
Total returns	384
Total rejected surveys	46
Final sample before screening	338
Final sample	291
Response rate	3.5%

On average, respondents held 11.18 years of experience in either the IT or IT security fields. Twenty-one percent of respondents are female and 79 percent male. Table 2 shows the position levels of respondents. As shown, 64 percent of respondents are at or above the supervisory level.

Table 2: Respondents' organizational level	Pct%
Senior Executive	1%
Vice President	1%
Director	20%
Manager	23%
Supervisor	19%
Associate/Staff	5%
Technician	26%
Contractor	5%
Total	100%

Table 3 shows the headcount (size) of respondents' business companies or government entities. As can be seen, 47 percent of respondents are employed by larger-sized organizations with more than 5,000 individuals.

Table 3: Headcount (size) of respondents' organizations?	Pct%
Less than 500	5%
500 to 1,000	11%
1,001 to 5,000	39%
5,001 to 25,000	28%
25,001 to 75,000	11%
More than 75,000	6%
Total	100%

Pie Chart 1 shows the industry sub-segments that best defines respondents' organizations. As can be seen, the largest sectors include private (46 percent) and public (22 percent) power utilities.

Pie Chart 1: Industry sub-segments of respondents' organizations

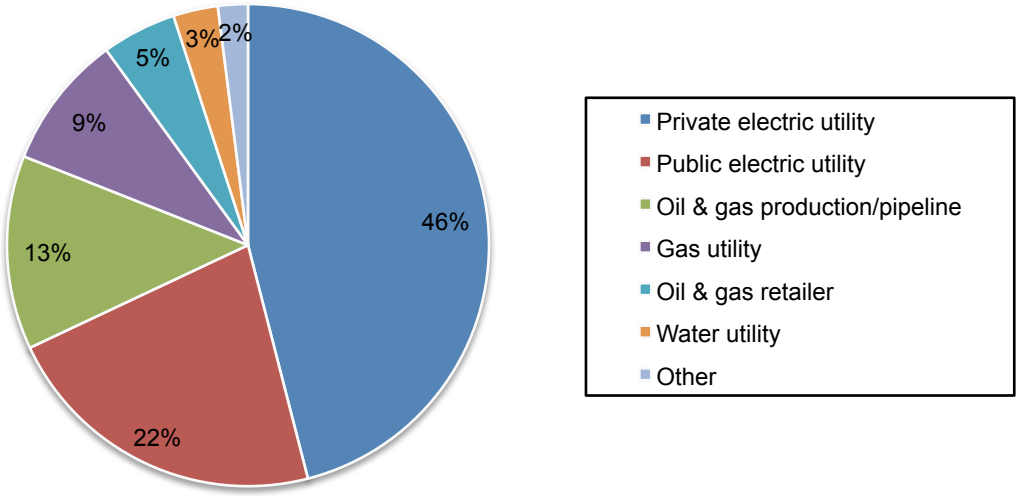


Table 4 reports the geographic footprint of respondents' organizations. In total, 56 percent of organizations have operations (headcount) in two or more countries. In addition, 41 percent have operations in one or more EMEA nations. Finally, a total of 18 percent have operations in all major regions of the world.

Table 4: Geographic footprint of respondents' organizations	Pct%
United States	100%
Canada	56%
Europe, Middle East & Africa	41%
Asia-Pacific	18%
Latin America (including Mexico)	23%

Part 4. Conclusion

We believe the findings show that energy and utilities organizations are struggling to identify the relevant issues that are plaguing their company from a security perspective. As an indication of their vulnerability, it takes an average of 22 days to detect insiders making unauthorized changes.

A barrier to closing this vulnerability and minimizing the risk is the fact that these organizations are not prioritizing IT security. In fact, the physical security budget is about *nine times* the information security budget. There is also the finding that preventing downtime is more critical than stopping a cyber attack.

Further, energy and utilities organizations either don't know, or are unsure what solutions are available to help overcome their security issues. Seventy-two percent say initiatives are not effective at getting actionable intelligence, and only thirty-nine percent are currently using a SIEM solution.

We believe the security of energy and utilities organizations needs to be addressed quickly if we are to prevent attacks and exploits that could disrupt the critical infrastructure. The solution is to make IT security a strategic initiative across the enterprise. Achieving a solid state of security will help organizations face the dual challenge of dealing with security threats and complying with regulatory and legal mandates.

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 IT and IT security practitioners, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that auditors who did not participate are substantially different in terms of underlying beliefs from those who completed the survey.
- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners in the utilities or energy industry. We also acknowledge that responses from paper, interviews or telephone might result in a different pattern of findings.
- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from respondents. While certain checks and balances were incorporated into our survey evaluation process, there is always the possibility that certain respondents did not provide responses that reflect their true opinions.

Appendix: Detailed Survey Responses

The following tables provide the frequencies or percentage frequencies of all survey responses. Please note that all information was collected in March 2011.

Sample response	Freq.
Sampling frame	8220
Total returns	384
Total rejected surveys	46
Final sample before screening	338
Final sample	291
Response rate	3.5%

Part 1. Screening

S1a. Is your present employer an organization in the utilities (electric, gas or water) or energy industry?	Freq.	Minus
Yes	331	
No	7	7
Total	338	

S1b. Does your job involve securing the organization's information assets, enterprise systems or the critical infrastructure? Please mark yes even if your job is only partially dedicated to the security function.	Freq.	Minus
Yes	315	
No	16	16
Total	331	

S1c. How familiar are you with NERC, FERC and CIP standards on the protection of cyber assets and the critical infrastructure?	Freq.	Minus
Very familiar	111	
Somewhat familiar	93	
Not familiar	87	
No knowledge	24	24
Total	315	47

Part 2. Attributions. Please rate each one of the following seven statements using the scale provided below each item.	Strongly agree	Agree
Q1a. My organization has sufficient resources to achieve compliance with leading security standards such as those prescribed by NERC or other regulatory authorities.	19%	31%
Q1b. My organization sees security as a strategic priority across the enterprise.	21%	23%
Q1c. My organization is proactive in managing security risks to information assets, enterprise systems, SCADA networks and critical infrastructure.	21%	20%
Q1d. My organization's security operations are dedicated to preventing or detecting advance persistent threats (APTs).	18%	21%
Q1e. My organization uses state-of-the-art technologies to minimize risks to SCADA networks.	15%	18%
Q1f. My organization's security operations are dedicated to protecting the nation's critical infrastructure.	13%	19%
Q1g. My organization views IT security as equally important to physical security.	16%	13%

Part 3: Operations in Europe, Middle East & Africa (EMEA)

Q2a. Does your organization have operations in the EMEA marketplace?	Pct%	
Yes	41%	119
No (Go to 3a)	59%	
Total	100%	

Please rate each one of the following six statements using the scale provided below each item.	Strongly agree	Agree
Q2b. Security and compliance initiatives within the energy industry are just as important, if not more important, across EMEA operations as they are for the United States.	33%	25%
Q2c. The threat level to the smart grid and SCADA networks in the United States is greater than EMEA because of web-enabled access to networks and enterprise systems.	34%	29%
Q2d. The threat level to the smart grid and SCADA networks in the United States is greater than EMEA because of lagging regulations and generally accepted compliance standards.	39%	33%

Q2e. Based on your organization's existing security posture, do you consider your business operations in the EMEA countries to be more vulnerable than your operations in the United States?	Pct%
Yes	21%
No	73%
Unsure	6%
Total	100%

Q2f. How does the present regulatory environment relating to the smart grid and SCADA networks affect your organization's security program in the United States?	Pct%
Negative impact	17%
No impact	60%
Positive impact	9%
Cannot determine	14%
Total	100%

Q2g. How does the present regulatory environment relating to the smart grid and SCADA networks affect your organization's security program in EMEA?	Pct%
Negative impact	6%
No impact	45%
Positive impact	29%
Cannot determine	20%
Total	100%

		291
Part 4. General security questions	Pct% Yes	Pct% No
Q3a. Does your organization consider security a priority?	40%	60%
Q3b. Do C-level executives fully understand and appreciate security initiatives?	29%	71%
Q3c. Are employees in your organization made aware of security requirements?	56%	44%
Q3d. Is compliance with security requirements strictly enforced?	51%	49%
Q3e. Is compliance with standards such as NERC a major security objective?	23%	77%
Q3f. Are corporate security (physical) and IT security (logical) functions integrated?	28%	72%
Q3g. Do security operations have clearly defined lines of responsibility and authority (parity)?	31%	69%

Q3h. Are contractors, vendors and other third parties held to high standards for security as a business condition?	39%	61%

Q4. What are the top security objectives or missions within your organization? Check only the top two choices.	Pct%
Prevent or quickly detect APTs	5%
Minimize risks and vulnerabilities	32%
Prevent cyber attacks	14%
Minimize downtime	55%
Comply with regulatory and legal mandates	38%
Secure the national critical infrastructure (including the smart grid)	9%
Improve the organization's security posture	31%
Improve the organization's relationship with business partners	6%
None of the above	10%
Total	200%

Q5. What are the top security threats that affect your organization? Check only the top two choices.	Pct%
Negligent insiders	43%
System glitches (including process failure)	36%
Malicious or criminal insiders	11%
Web-based attacks	9%
Insecure web applications	40%
Insecure endpoints	26%
Insecure smart meters	5%
Third party mistakes or flubs (including cloud providers)	11%
Denial of service (DNS) attacks	3%
Electronic agents such as viruses, worms, malware, botnets and others	9%
Nation-state, terrorist or criminal syndicate sponsored attacks	5%
Other (please specify)	2%
Total	200%

Q6. Where is data (information assets) most susceptible to loss or theft? Please select only the top two choices.	Pct%
Applications	43%
Databases	12%
Storage devices	15%
Servers	9%
Networks	47%
In-transit	6%
Laptops and desktops	26%
Data capture devices (including smart meters)	7%
Mobile devices (including smartphones)	11%
Third parties (including cloud providers)	12%
Backup media	2%
Paper documents	2%
Other (please specify)	8%
Total	200%

Q7. Who is **most responsible** for ensuring security objectives are achieved? Please select one best response.	Pct%
CEO	0%
CFO	2%
CIO	15%
CTO	5%
IT security leader (CISO)	9%
Security leader (CSO)	18%
Compliance	6%
Law department	3%
Business unit leaders	5%
Facilities or data center management	8%
No one role has overall responsibility	29%
Other (please specify)	0%
Total	100%

Part 4. Security compliance requirements

Following are well-known security requirements as defined by cyber security standards, including those espoused by NERC and other related initiatives. For each requirement, please rate: (1) relative difficulty your organization has in achieving each security objective and (2) level of importance in achieving each security objective.	Very difficult & difficult	Critical & very important
Q8a. Protect SCADA systems	96%	96%
Q8b. Protect sensitive or confidential information at rest (in storage)	75%	69%
Q8c. Encrypt transmission of sensitive or confidential information across open, public networks (such as smart meter communication with the smart grid).	76%	70%
Q8d. Use and regularly update anti-virus software	48%	85%
Q8e. Develop and maintain secure systems and applications	82%	78%
Q8f. Restrict access to confidential information on a need-to-know basis.	49%	54%
Q8g. Restrict physical access to critical assets.	47%	85%
Q8h. Track and monitor all access to information assets, enterprise systems, SCADA networks and critical infrastructure.	52%	55%
Q8i. Regularly test security readiness in terms of systems and processes.	67%	52%
Q8j. Maintain comprehensive policies that address information and physical security requirements.	36%	50%

Part 5. Most effective security technologies & control practices

Q9. Following are technologies that foster security objectives and compliance with standards. For each item, indicate the **effectiveness** of each technology with respect to achieving security objectives by using one of three choices: high, moderate or low effectiveness, respectively.	**Are you using this?**	
Technologies used to achieve compliance	**Yes**	**High**
Access governance systems	26%	44%
Anti-virus / anti-malware solution	99%	78%
Code review	34%	23%
Event management systems (SIEM)	39%	47%
Data loss prevention systems	19%	21%
Database scanning	38%	45%
Database activity monitoring (DAM)	24%	46%
Encryption of data at rest	54%	50%
Encryption of data in motion	58%	52%
Endpoint encryption solutions	23%	48%
Firewalls	100%	79%
ID & credentialing system	48%	45%
Identity & access management systems	45%	49%
Intrusion detection or prevention systems	60%	55%
Perimeter or location surveillance systems	67%	62%
Network or traffic intelligence systems	28%	43%
Virtual privacy network (VPN)	49%	49%
Web application firewalls (WAF)	23%	50%
Website sniffers or crawlers	12%	23%

Q10. Following are control practices that foster security objectives and compliance with standards. For each item, indicate the **effectiveness** of each practice with respect to achieving security objectives by using one of three choices: high, moderate or low effectiveness, respectively.	**Are you doing this?**	
Control practices to achieve compliance	**Yes**	**High**
Business continuity and disaster recovery	100%	85%
Training of end users	88%	46%
Frequent IT audits	10%	57%
Training of security practitioners	51%	43%
Redress & enforcement	62%	57%
Background checks of privileged users	86%	59%
Secure disposal of paper documents	70%	23%
Upstream communications	22%	12%
Safe disposal of electronic data-bearing devices	31%	25%
Control assessment	45%	40%
Vetting & monitoring of third parties	49%	44%
Annual external audit	19%	19%
Standardization	38%	46%
Record retention & archive management	41%	30%
Certification of security staff	59%	59%
Monitoring regulatory changes	6%	10%
Quality assurance	6%	15%
Helpdesk activities	69%	28%
Policies & procedures	98%	63%
Surveillance & manual inspection	50%	71%

Part 6. Exploits & security breaches

Q11a. How often has your organization suffered a security breach by way of exploit or data breach over the past 12 months?	Pct%
None (go to Q12)	24%
1 incident	48%
2 to 5 incidents	13%
More than 5 incidents	9%
Cannot determine	6%
Total	100%

Q11b. To the best of your knowledge, what was the root cause of the security breaches experienced by your company over the past 12 months? Please select all that apply.	Pct%	221
External attack	12%	
Insider attack	5%	
Combined external and insider attack	0%	
Accidental loss (negligence)	28%	
Malicious code	11%	
Virus, worms, Trojans, malware or botnets	7%	
Abuse by privileged IT staff	8%	
Abuse by outside vendors or business partners	16%	
Ex-filtration (attack from the inside)	2%	
Do not know	11%	
Total	100%	

Q11c. What core systems were compromised as a result of the security breaches experienced by your company over the past 12 months? Please select all that apply.	Pct%
CRM applications	0%
HR applications	2%
Data capture/POS	4%
SCADA networks	5%
Servers	8%
ERP applications	25%
Storage devices	27%
Endpoints	52%
Databases	56%
Unsure	5%
Total	199%

Q11d. Approximately (best guess), what is the total cost to your organization as a result of security breaches experienced over the past 12 months?	Pct%
Less than $10,000	16%
$10,001 to $50,000	21%
$50,001 to $100,000	15%
$100,001 to 500,000	24%
$500,001 to $1,000,000	3%
More than $1,000,000	1%
Cannot determine	2%
Total	100%
Extrapolated average cost	$156,663

Q12. How do you define an offense (attack) on your network?	Pct%	291
Any network probe	71%	
Data manipulation/data theft	86%	
Information copied or downloaded without authorization	35%	
Data being accessed without authorization	59%	
Access to information by any individual without proper credentials or a "need-to-know."	64%	
Other (please specify)	9%	
Total	324%	

Q13. What is the likelihood of a successful exploit on your organization's network over the next 12 months?	Pct%
Very likely	23%
Likely	46%
Somewhat likely	15%
Not likely	11%
No chance	5%
Total	100%

Q14. Approximately how long would it take your organization to detect an insider who made some type of unauthorized change or committed some sort of malicious activity?	Pct%
Immediately (less than one hour)	6%
A few hours	15%
A few days	14%
A few weeks	11%
A few months	4%
More than a few months	15%
Cannot determine	35%
Total	100%
Extrapolated number of days	22.06

Q15. Approximately what percentage of your network components, including third-party endpoints such as smart phones and home computers, are outside the direct control of your organization's security operations?	Pct%
Less than 10 percent	16%
10 to 25 percent	20%
26 to 50 percent	17%
51 to 75 percent	10%
More than 75 percent	5%
Cannot determine	32%
Total	100%
Extrapolated percent of network components outside direct control	30%

Q16. Are there certain areas of your network that present the highest level of threat or vulnerability to your organization? Please only provide your top two choices.	Pct%
Servers	8%
Routers/switches	6%
Applications	44%
Databases	38%
Mobile devices	35%
Storage devices	16%
Backup devices	5%
Email servers	13%
Endpoints	34%
Other (please specify)	1%
Total	200%

218

Q17. Do you feel your organization's existing security controls provide adequate levels of protection against attacks and exploits occurring through smart meters and smart grid systems?	Pct%	Revised
Yes	16%	21%
No	35%	47%
Unsure	24%	32%
Not applicable. We are not connected to the smart grid	25%	0%
Total	100%	100%

Q18. With respect to the security of your organization's critical infrastructure, what best describes your level of concern about third-party providers who are or will soon be connected to the smart grid.	Pct%	Revised
Very concerned	31%	41%
Somewhat concerned	20%	27%
Not concerned	24%	32%
Not applicable. We are not connected to the smart grid	25%	0%
Total	100%	100%

Part 7. Other questions

Q19. In terms of your organization's security objectives or mission, how important is compliance with NERC security guidelines?	Pct%	Revised
Most important	9%	12%
Important	19%	25%
Somewhat important	28%	37%
Not important	19%	25%
Not applicable. We are not subject to NERC	25%	0%
Total	100%	100%

Q20a. How does your organization participate in the smart grid?	Pct%
Fully responsible for implementation and ongoing operations	36%
Partially responsible for implementation and ongoing operations	21%
Not responsible for implementation and ongoing operations	9%
Not applicable. We do not participate in the smart grid	29%
Unsure	5%
Total	100%

Q20b. [If fully or partially responsible for smart grid implementation and operations] What steps does your organization take to secure the smart grid?	Pct%	166
Ensure smart meter devices are secure	35%	
Monitor suspicious traffic from the smart meter to the utility	28%	
Limit access to consumer or energy consumption data	32%	
Limit physical access to third parties	45%	
Firewall electronic access	43%	
Educate consumers	9%	
Other (please specify)	5%	
No new steps	39%	
Unsure	34%	
Total	270%	

Q21a. What dollar range best describes your organization's IT security budget in the present fiscal year?	Pct%	291
Less than $1 million	21%	
Between $1 to 2 million	32%	
Between $2 to $4 million	16%	
Between $4 to $6 million	13%	
Between $6 to $8 million	11%	
Between $8 to $10 million	3%	
Between $10 to $12 million	1%	
Between $12 to $14 million	1%	
Between $14 to $16 million	2%	
Between $16 to $18 million	0%	
Between $18 to $20 million	0%	
Over $20 million	0%	
Total	100%	
Total IT security budget ($1,000,000 omitted)	3.358	

Q21b. What dollar range best describes your organization's physical (plant or facilities) security budget in the present fiscal year?	Pct%
Less than $1 million	0%
Between $1 to 2 million	1%
Between $2 to $4 million	3%
Between $4 to $6 million	5%
Between $6 to $8 million	4%
Between $8 to $10 million	6%
Between $10 to $12 million	1%
Between $12 to $14 million	0%
Between $14 to $16 million	9%
Between $16 to $18 million	4%
Between $18 to $20 million	6%
Between $20 to $40 million	29%
Over 40 million	32%
Total	100%
Total IT security budget ($1,000,000 omitted)	27.235

Q22. How effective are your organization's security initiatives in terms of providing actionable intelligence (such as real-time alerts, threat analysis and prioritization) about actual and potential exploits?	Pct%
Very effective	9%
Somewhat effective	19%
Not effective	22%
We do not get real-time alerts, threat analysis and threat prioritization	50%
Total	100%

Q23a. Has your organization deployed SIEM?	Pct%	113
Yes	39%	
No	61%	
Total	100%	

Please rate the following statement using the scale provided below.	Strongly agree	Agree
Q23b. SIEM helps to bridge gaps among departments such as IT operations, network operations, data center management, and others.	41%	32%

Q24. Has your organization deployed log management?	Pct%	291
Yes	46%	
No	56%	
Total	102%	

Q25. Please rank order the following six security priorities from 6 = highest priority to 1 = lowest priority.	Average rank	Order
Securing smart meters	1.21	6
Protecting SCADA networks	5.06	1
Securing information assets	3.91	4
Protecting enterprise systems	4.82	2
Protecting endpoints to the network	4.03	3
Protecting the nation's critical infrastructure	0.22	7
Average	3.21	5

Part 8. Your role

D1. What organizational level best describes your current position?	Pct%
Senior Executive	1%
Vice President	1%
Director	20%
Manager	23%
Supervisor	19%
Associate/Staff	5%
Technician	26%
Contractor	5%
Other (please specify)	0%
Total	100%

D2. Check the **Primary Person** you or your IT security leader reports to within the organization.	Pct%
CEO/executive committee	1%
Chief financial officer	2%
General counsel	0%
Chief information officer	43%
Chief technology officer	4%
IT security leader	10%
Facility or plant management	13%
Compliance leader	6%
Human resource leader	0%
Security officer	15%
Chief risk officer	5%
Other (please specify)	1%
Total	100%

D3. What best describes your organization's industry segment?	Pct%
Private electric utility	46%
Public electric utility	22%
Gas utility	9%
Water utility	3%
Oil & gas exploration	0%
Oil & gas production/pipeline	13%
Oil & gas retailer	5%
Alternative energy	0%
Other	2%
Total	100%

D4. Experience level	Mean	Median
Total years of IT or security experience	11.18	10.50
Total years in present position	5.80	5.00

D5. Gender	Pct%
Female	21%
Male	79%
Total	100%

D6. Where are your employees located? (check all that apply):	Pct%
United States	100%
Canada	56%
Europe, Middle East & Africa	41%
Asia-Pacific	18%
Latin America (including Mexico)	23%

D7. What is the worldwide headcount of your organization?	Pct%
Less than 500	5%
500 to 1,000	11%
1,001 to 5,000	39%
5,001 to 25,000	28%
25,001 to 75,000	11%
More than 75,000	6%
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 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.