# Energy Industry Cybersecurity Report

July 2015

Smart. Focused. Done Right.®

scottmadden
MANAGEMENT CONSULTANTS

## INTRODUCTION

Due to information sharing concerns, energy industry cybersecurity information is not readily available. However, understanding what your industry peers are doing to respond to a growing cyber threat is required to make the best possible decisions.

ScottMadden is committed to serving the energy community by providing timely cybersecurity information. We provide daily research report updates, statistics, and industry insight on our sponsored website, www.gridcybersec.com. Cybersecurity leading practices and recommendations can be found at www.scottmadden.com. And we are pleased to provide this Energy Industry Cybersecurity Report, a compilation of energy sector cybersecurity research.

This report will help you understand:

- Industry perceptions of cyber risks
- Industry confidence levels in its ability to mitigate these risks
- Cybersecurity strategies, organizational responsibilities, and practices being used
- Cybersecurity concerns and obstacles that need to be addressed in order to adequately secure their critical assets

This report will help you evaluate your cybersecurity program efforts, including:

- How your practices and capabilities compare to the industry
- How your perceptions and concerns compare to the industry

ScottMadden's research is gathered from global energy industry surveys. Information on SCADA and industrial control systems is pulled from surveys of critical infrastructure operators that include energy utilities (but not exclusively).

## KEY FINDINGS

The report's key findings include:

- Energy organizations acknowledge a growing cybersecurity risk, and most expect their IT and operation technology (OT) assets to be attacked
- Most organizations have implemented cybersecurity programs and consider them relatively mature
- Organizations are not confident they are effectively managing risks to their IT and OT assets

- Most organizations have experienced a cybersecurity incident that resulted in either a data loss or disruption to operations
- Insiders present the biggest cybersecurity risk to organizations
- Organizations are concerned about having sufficient cybersecurity resources
- Most organizations share responsibility for OT security between the information security officer and the operator of the control system
- Organizations are lacking real-time, actionable cybersecurity intelligence
- Half of the organizations have adopted a unified security and controls framework

These findings reveal some inconsistencies. There is growing awareness of cybersecurity risks and the increasing threat they present to energy operations. Organizations also claim their cybersecurity practices are maturing. But despite this improved awareness and these maturing cyber capabilities, there is not a corresponding level of confidence in the organization's ability to deal with security risks.

There are lessons to be learned from the incidents that are occurring. While nation-state, terrorist, and criminal activities get all the headlines, the number-one threat remains insiders and trusted partners. Your cybersecurity efforts need to be commensurate with this high-probability risk. The research identified relatively flat security budgets, so it is important that security efforts and investments are focusing on high-probability and high-impact risks.

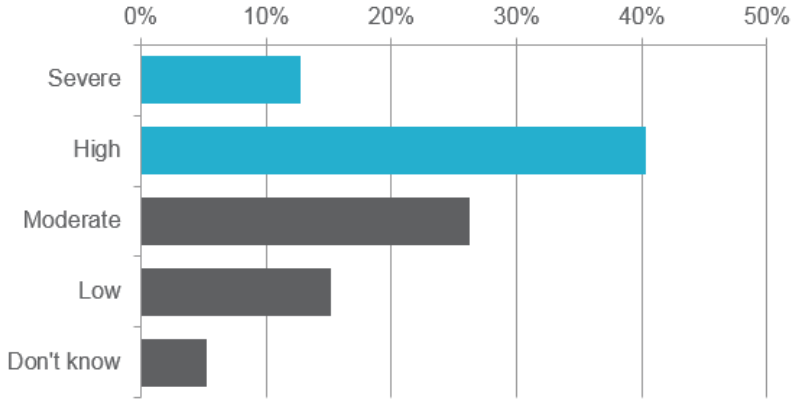
A number of improvement opportunities are also identified. This includes improvements in real-time, actionable intelligence. Adoption of a standard control framework, preferably the NIST cybersecurity framework, can also guide efforts for the roughly 50 percent of organizations not using an industry standard. There is also an opportunity to dedicate resources explicitly to OT cybersecurity, including SCADA and industrial control systems.

## FINDINGS DETAILS

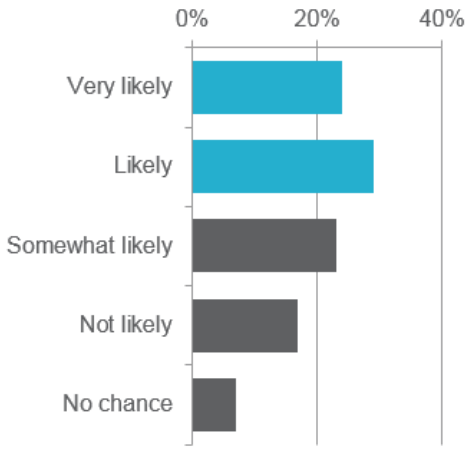
### Finding 1: Energy organizations acknowledge a growing cybersecurity risk, and most expect their IT and OT assets to be attacked.

Organizations indicated that the risk level of their control system environments has substantially increased, and they anticipate an attack on their IT and SCADA assets.

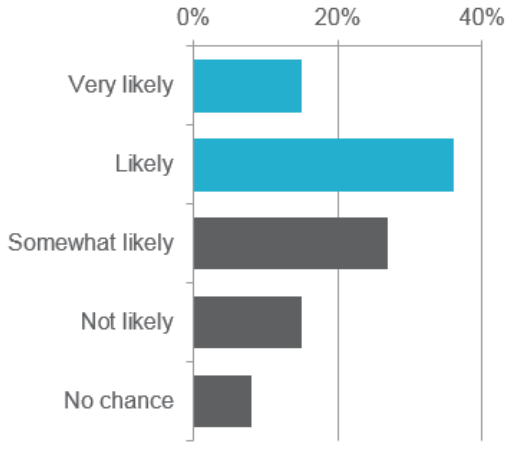
**What is the perceived magnitude of cybersecurity threats to your control systems? [2]**




**What is the likelihood of an attack on your IT systems in the next 24 months? [1]**

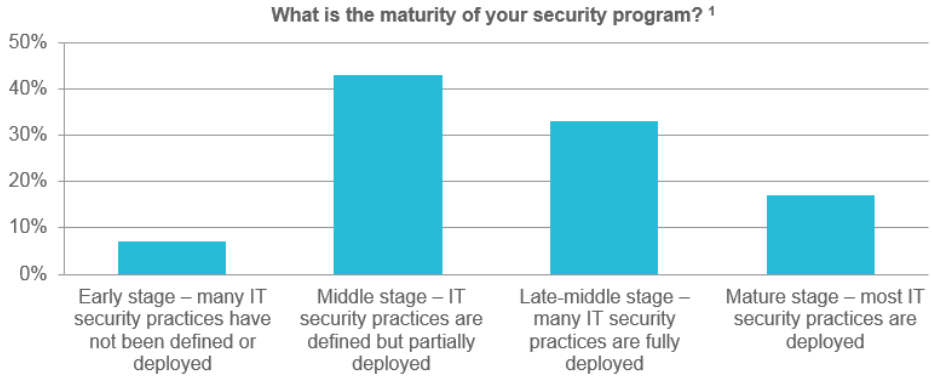


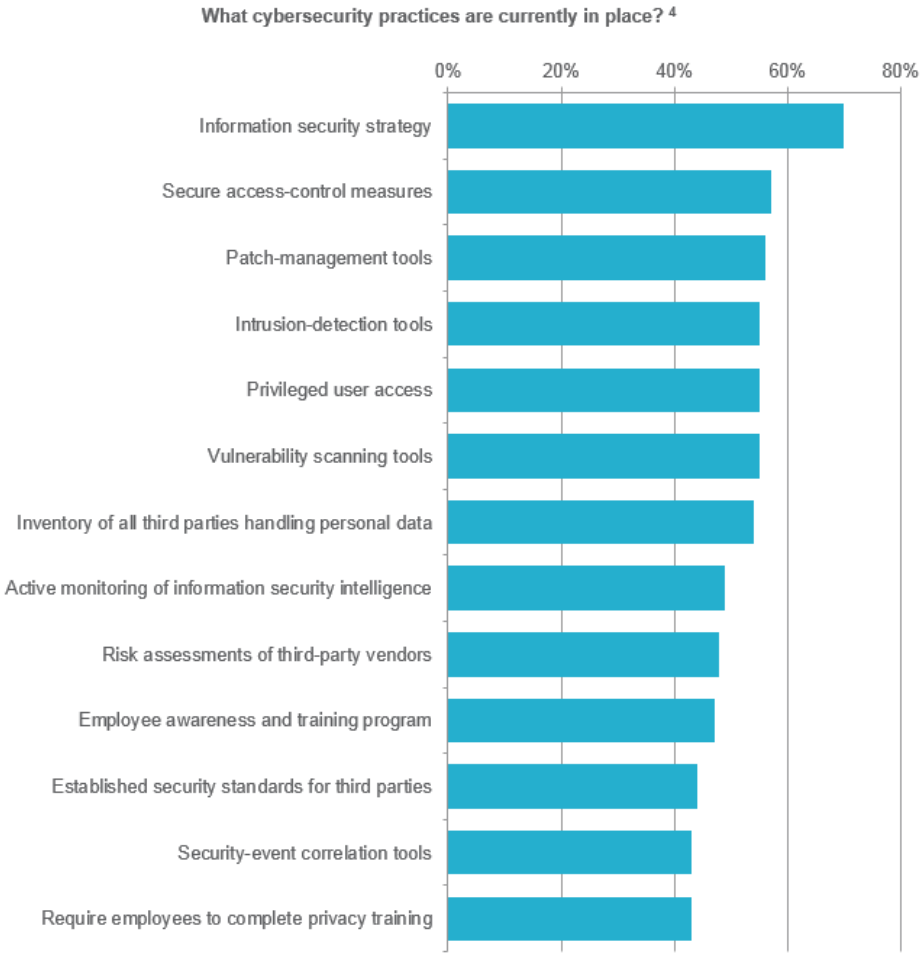

**What is the likelihood of an attack on your SCADA systems in the next 24 months? [1]**



**Finding 2: Most organizations have implemented cybersecurity programs and consider them relatively mature.**

The majority of organizations have many cybersecurity program elements in place, and the average maturity of industry security programs is considered middle to late stage—practices are defined and are either partially or mostly implemented.

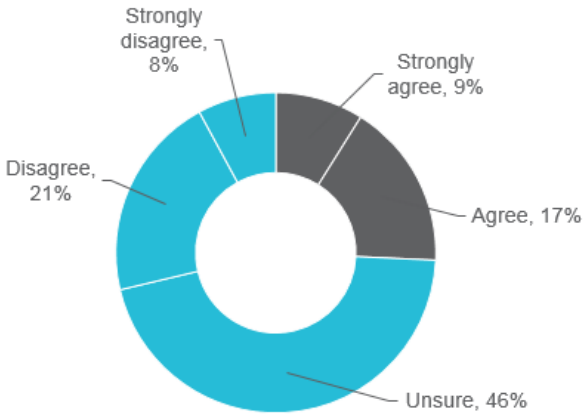


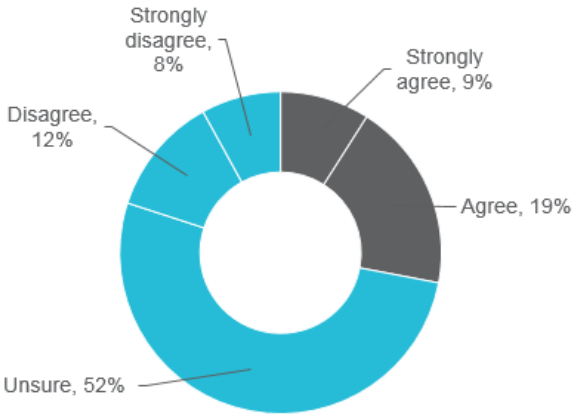
**Finding 3: Organizations are not confident they are effectively managing risks to their IT and OT assets.**

Organizations are unsure how effective their security management efforts are at mitigating risks. Specifically, they indicated weaknesses in compliance efforts, security requirement enforcement, and their use of state-of-the-art technologies.

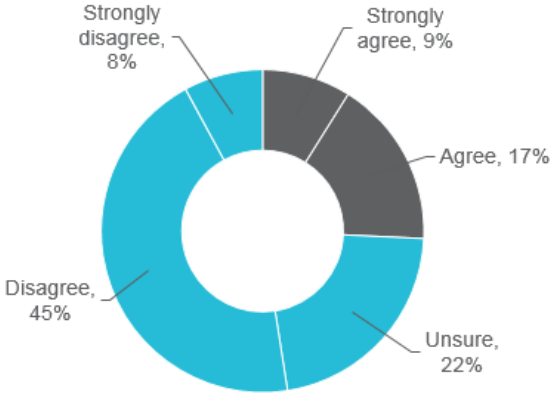
**My organization effectively manages security risks to information assets, enterprise systems, SCADA networks and critical infrastructure[1]**



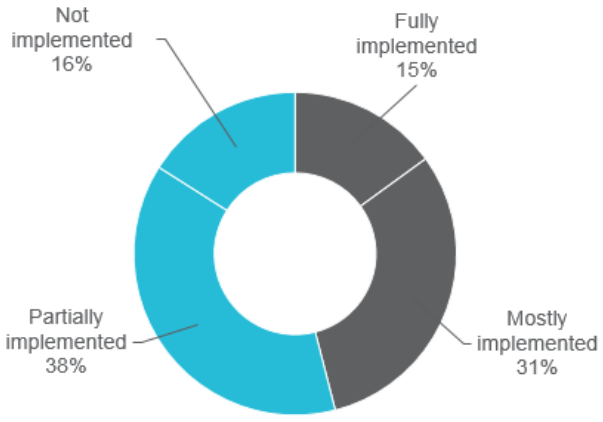

**Security and compliance industry initiatives enhance the security posture of my organization[1]**




**My organization uses state-of-the-art technologies to minimize security risks to SCADA networks and industrial control systems [1]**

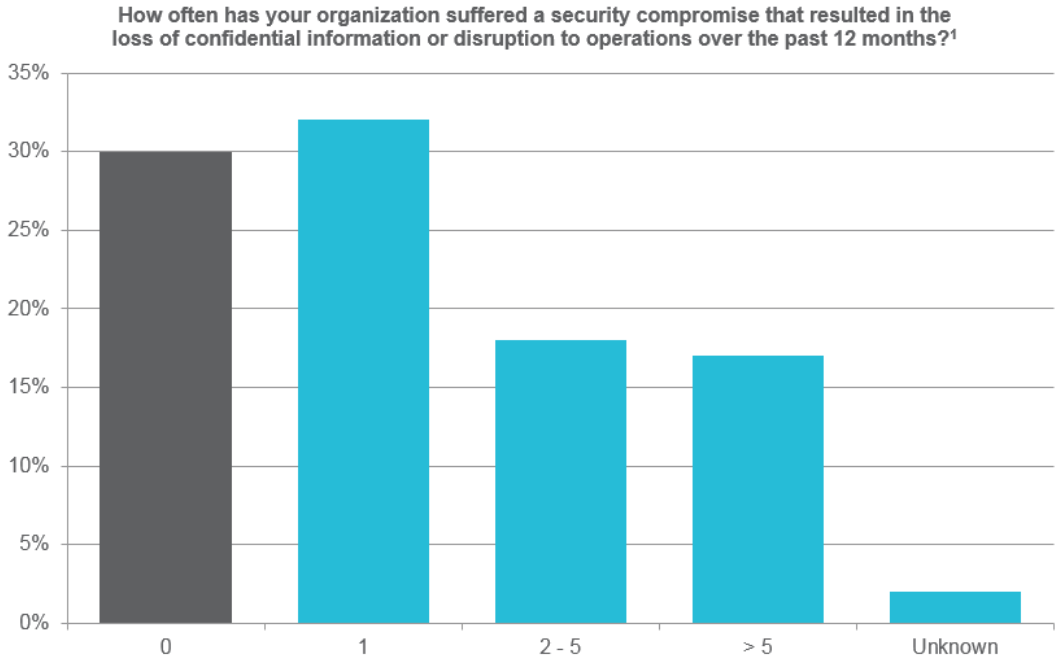



**Compliance with security requirements is strictly enforced [1]**



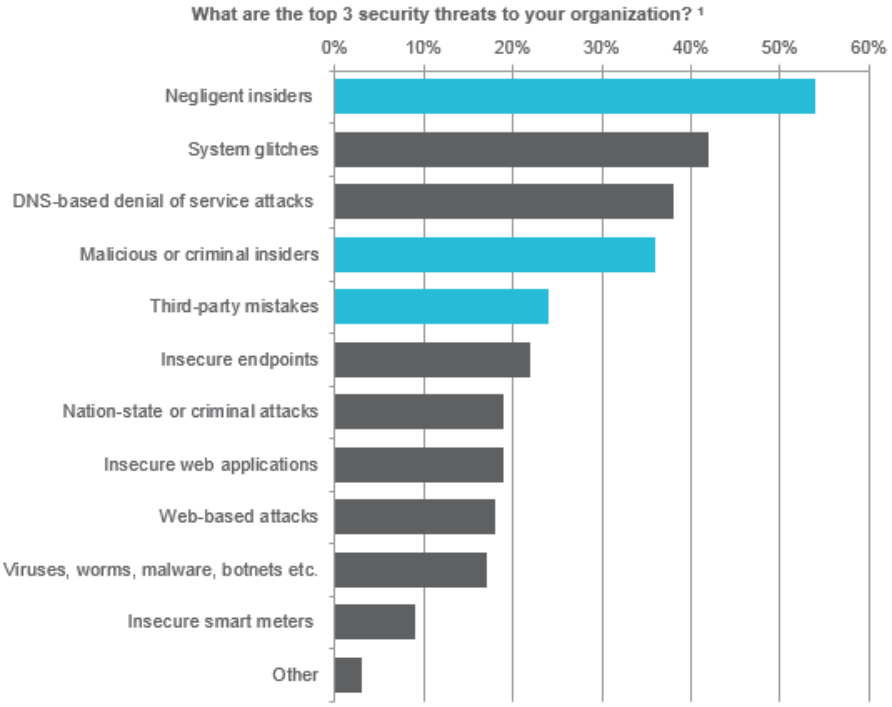
**Finding 4: Most organizations have experienced a cybersecurity incident that resulted in either a data loss or disruption to operations.**

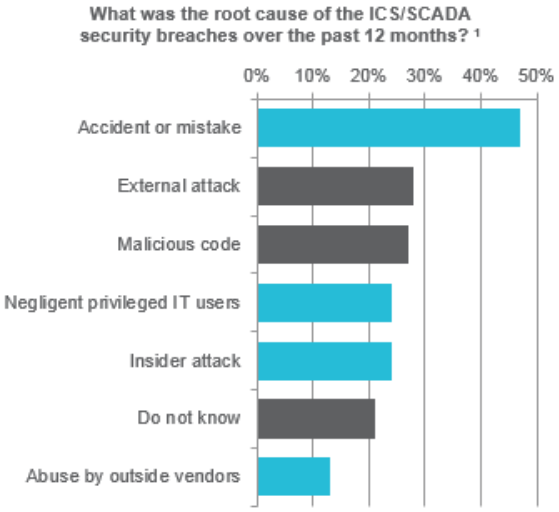
Two-thirds of organizations have experienced at least one disruptive cybersecurity incident. Thirteen percent have had their SCADA networks compromised, and 26 percent have had other industrial control systems impacted.[1]

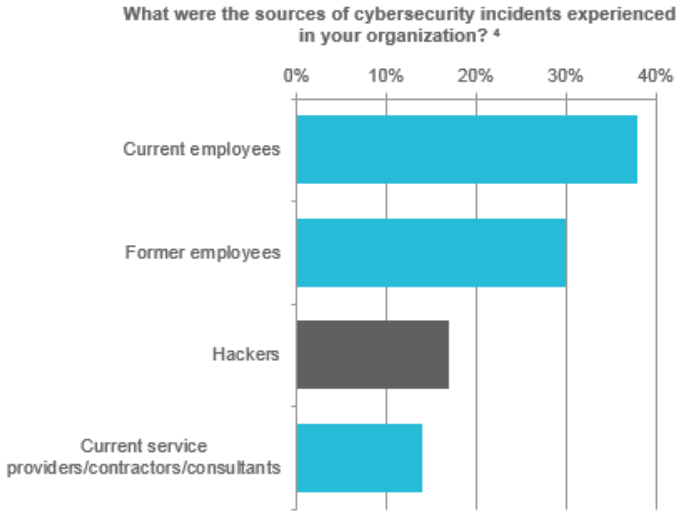


**Finding 5: Insiders present the biggest cybersecurity risk to organizations.**

Despite the well-publicized risks of nation-states, criminal enterprises, and hacktivists, insiders remain the most probable source of cyber risk—either intentionally or unintentionally.

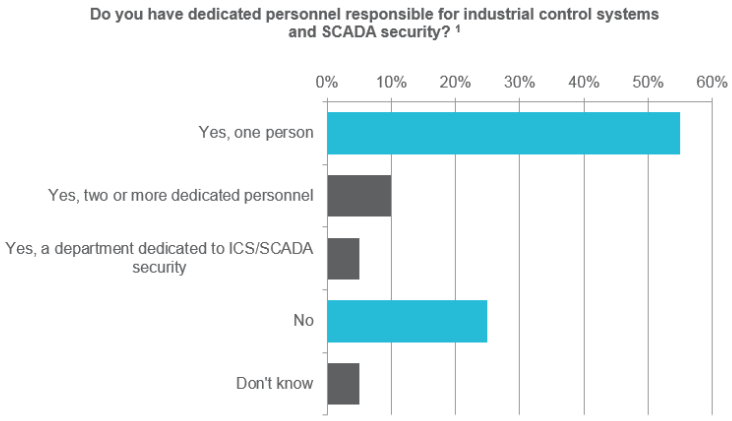


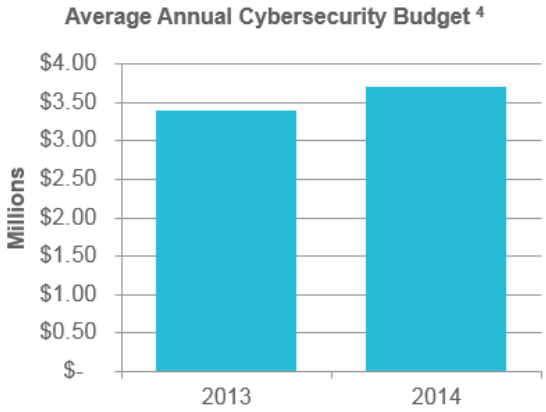



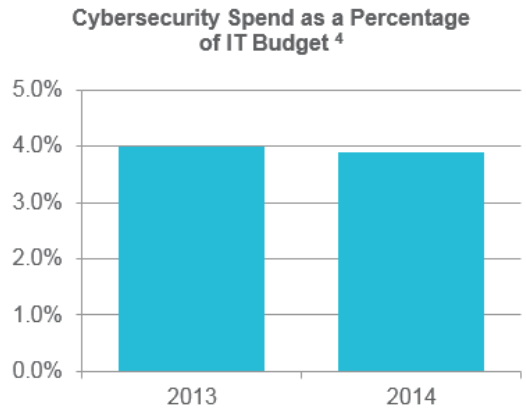



## Finding 6: Organizations are concerned about having sufficient cybersecurity resources.

Eighty percent of respondents indicated they have either one person or no one dedicated to control system cybersecurity, and spending has been flat while the perceived threat is increasing.

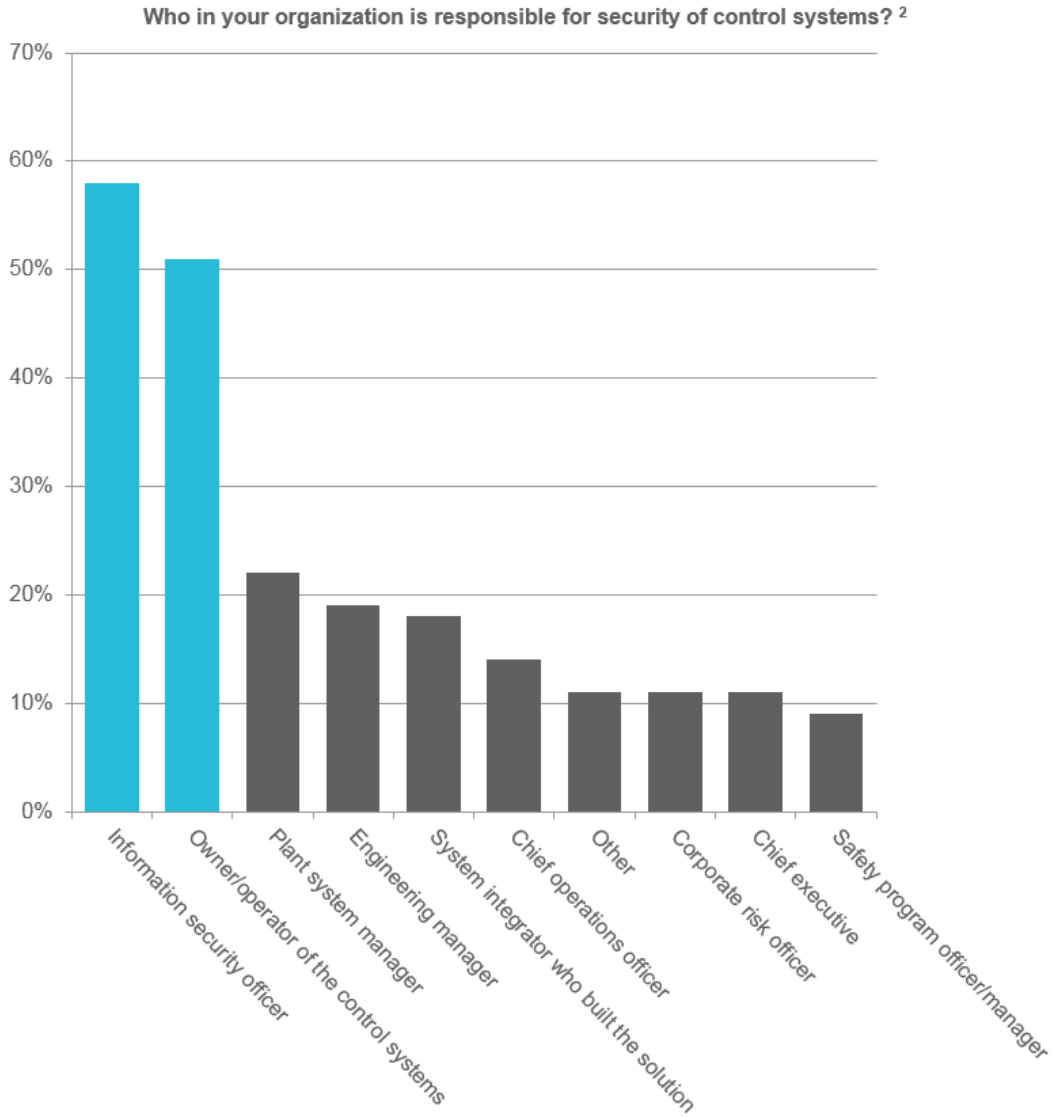



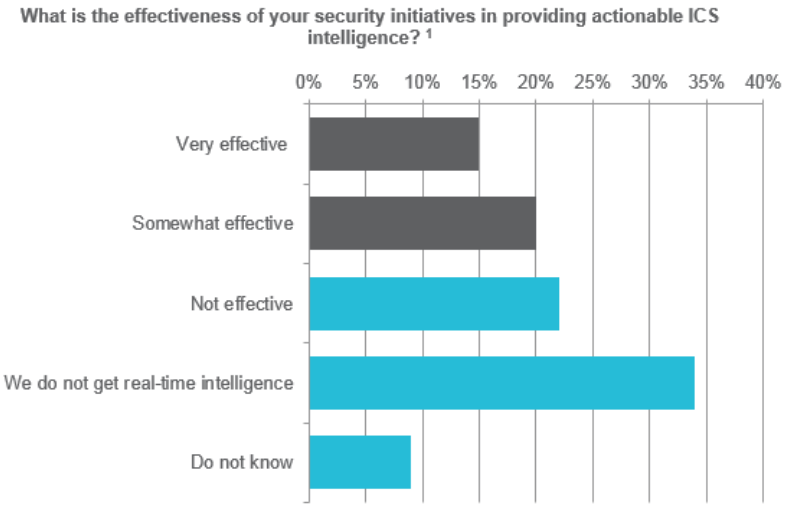
**Finding 7: Most organizations share responsibility for OT security between the information security officer and the operator of the control system.**

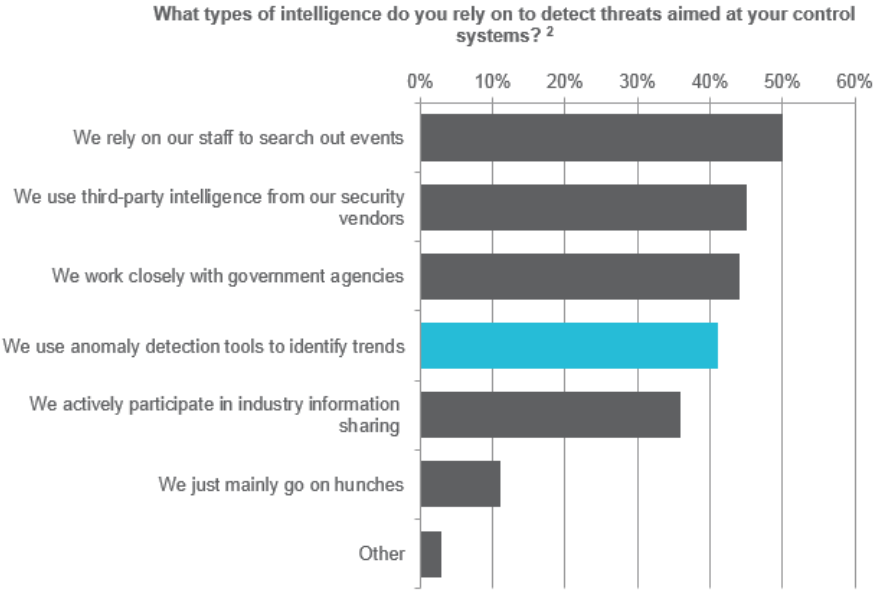
Control system operators were identified by just more than half of organizations surveyed as responsible for ICS cybersecurity. Few organizations have dedicated OT cybersecurity resources.



**Finding 8: Organizations are lacking real-time, actionable cybersecurity intelligence.**

Twenty-five percent of organizations characterized their OT intelligence as either very effective or effective, while 56 percent either indicated their intelligence as not effective or nonexistent. This is further demonstrated by the answers to incident questions, where a commonly provided answer was "unknown."

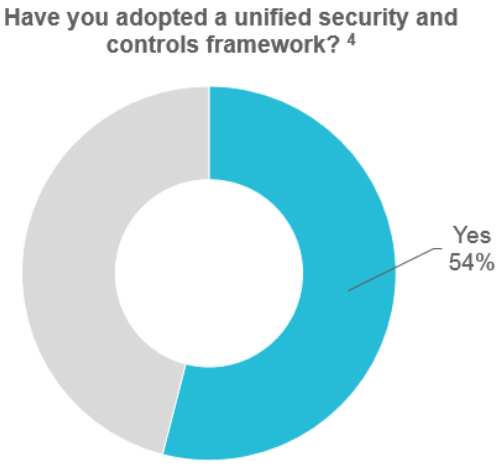


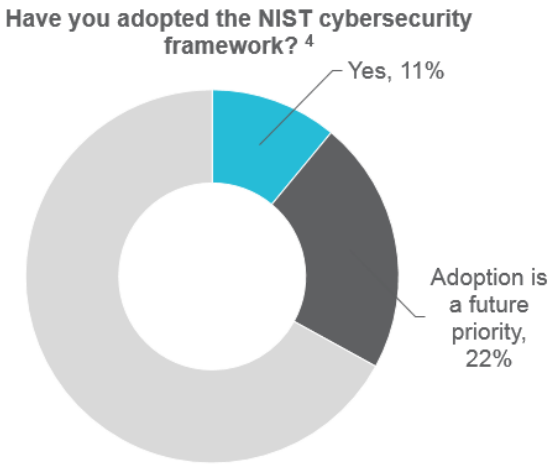




| Question | % Responding "Unknown" |
|---|---|
| What was the root cause of the ICS/SCADA security breaches over the past 12 months? [1] | 21% |
| If you had an ICS/SCADA breach, how many times did such events occur in the past 12 months? [2] | 34% |
| How long did it take to discover the ICS/SCADA infiltration or exploit? [2] | 34% |
| Source of ICS-CERT reported security incidents [3] | 38% |

**Finding 9: Half of the organizations have adopted a unified security and controls framework.**

One-third of organizations have either adopted or plan to adopt the NIST cybersecurity framework.




## CONCLUSIONS

Energy company responses to a growing cybersecurity threat have varied. Many capital projects have been launched, introducing new monitoring, detection, protection, and security management capabilities. Cybersecurity capabilities are perceived as maturing.

But this research shows that organizations are not becoming more confident in their ability to secure their critical assets. As more attention is placed on what the industry is doing, it is clear that new approaches are needed. This includes a more strategic approach to cybersecurity:

- Understanding the enterprise security risks to your organization's mission
- Focusing your organization's response on the highest priority risks
- Building foundational capabilities and methodically maturing and improving them
- Demonstrating tangible progress

## ABOUT SCOTTMADDEN'S ENERGY PRACTICE

We know energy. Since 1983, we have been consulting to the energy industry. We have served more than 300 clients, including 20 of the top 20 energy utilities. We have performed more than 2,400 projects across every energy utility business unit and every function. We have helped our clients develop strategies, improve operations, reorganize companies, and implement initiatives. Our broad and deep energy utility expertise is not theoretical—it is experience based.

## ABOUT THE AUTHOR

Jon Kerner leads ScottMadden's IT practice. Contact him at jkerner@scottmadden.com.

## FOR MORE INFORMATION

Please visit www.scottmadden.com to learn more about the services we offer.

Visit www.gridcybersec.com and subscribe to our newsletters to receive daily cybersecurity research. Also, follow us on twitter @gridcybersec.

[1] Critical Infrastructure: Security Preparedness and Maturity, Ponemon Institute, http://www.unisys.com/insights/critical-infrastructure-security

[2] Breaches on the Rise: A SANS Survey, SANS Institute, http://www.sans.org/reading-room/whitepapers/analyst/breaches-rise-control-systems-survey-34665

[3] ICS-CERT in Review: 2014, Industrial Control Systems Cyber Emergency Response Team, https://ics-cert.us-cert.gov/sites/default/files/documents/Year_in_Review_FY2014_Final.pdf

[4] Global State of Information Security Survey: 2015 (Power and Utilities), PWC, http://www.pwc.com/gx/en/consulting-services/information-security-survey