Market Watch

Cybersecurity in the Energy Industry

Companies Lack Confidence Despite Improvement

By Jon Kerner

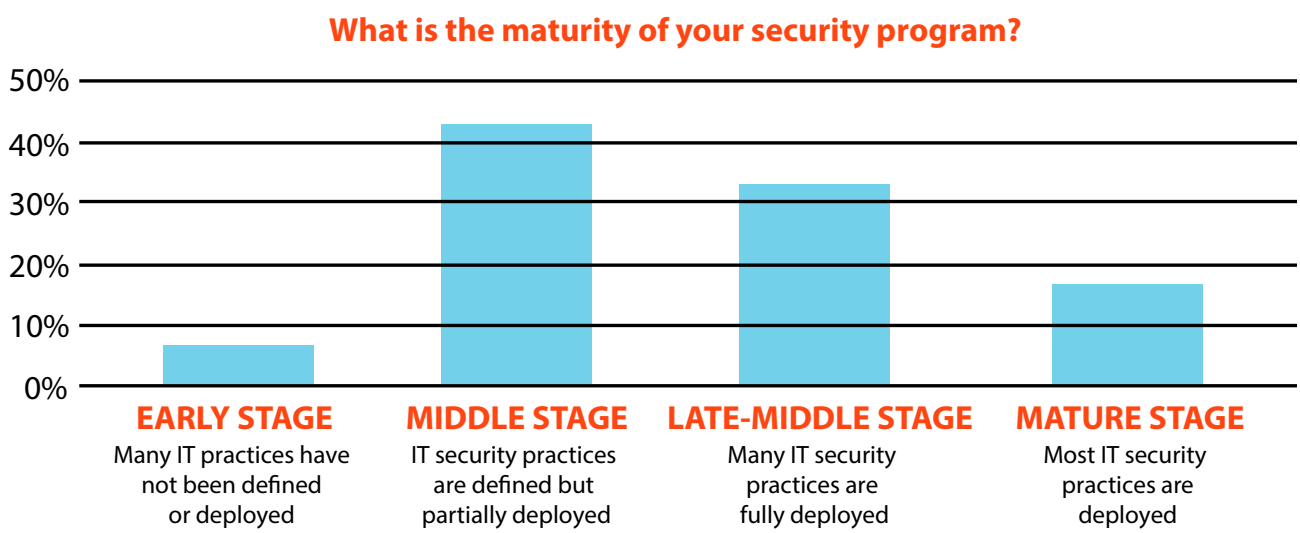

Figure 1

Source: Ponemon Institute

Energy organizations are lacking confidence in their cybersecurity preparation despite recent improvements in capabilities. ScottMadden, a management consulting firm specializing in the energy industry, recently released its research findings in its "Energy Industry Cybersecurity Report." What follows is a summary of their findings.

The energy industry has been successful in its efforts to raise awareness of the threat of cyber risks to critical infrastructure. When surveyed, most respondents characterize the risk as either severe or high, and many expect their IT and OT systems will be attacked within the next two years.

As a result, many dollars, and much time and attention, have been deployed to manage cybersecurity risks. Most organizations have implemented cybersecurity programs, and they consider them relatively mature (see Figure 1). Two thirds of organizations have cybersecurity strategies in place. More than half have implemented a variety of technical controls, including access controls, intrusion detection and patch management tools. In addition, more than 40 percent have implemented non-technical safeguards including risk assessments, employee awareness training and security standards.

Yet most organizations are not confident that they are prepared to address cybersecurity risks (see Figure 2). Only 26 percent believe that they effectively manage risks to information assets, enterprise systems, SCADA networks and critical infrastructure. Just 28 percent believe that industry security and compliance initiatives enhance the security posture of their organization, and less than half believe compliance with security requirements is strictly enforced within their organization.

Our research identified four reasons for this confidence gap:

1. Most organizations have already experienced a cybersecurity incident.
2. Many are concerned about having sufficient cybersecurity resources.
3. Organizations lack real-time, actionable cybersecurity intelligence.
4. Only half of the organizations have adopted a unified security and controls framework.

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

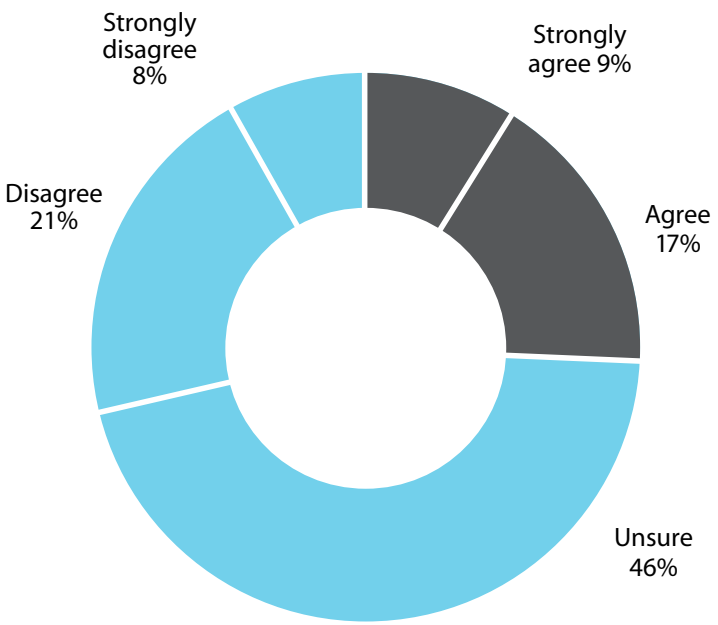

Figure 2

Source: Ponemon Institute

Cybersecurity Shortcomings

Despite cybersecurity preparation efforts, most organizations surveyed have experienced a cybersecurity incident resulting in either a data loss or disruption to operations. This includes 26 percent that had industrial control systems impacted and 13 percent that had their SCADA networks compromised.

Organizations are also feeling the burden of this increasing threat, in the form of heightened expectations. Yet less than a third of organizations indicated they had sufficient cybersecurity resources to comply with cybersecurity standards and requirements, and less than 20 percent have more than one person dedicated to control system cybersecurity.

Cybersecurity tactics have evolved from simply securing the perimeter with firewalls. Organizations must deal with the prospect that threats currently exist within their network. Therefore, actionable intelligence about anomalies within network environments has become increasingly important. This is particularly true with insider threats, i.e., risks from users with authorized access to network resources. Our re-

search revealed that insiders, not hackers, represent the biggest cyber threat to organizations. Yet most organizations indicated they lack real-time, actionable cybersecurity intelligence. Fifty-six percent of respondents indicated their intelligence is either not effective or nonexistent, and most do not use anomaly detection tools. This lack of insight into cybersecurity incident activity is further demonstrated by responses to questions about these incidents. When asked about details of recent cybersecurity incident activity, depending on the question, 20 percent to almost 40 percent of respondents provided a response of "unknown."

Organizing cybersecurity programs around a unified security framework is widely seen as a proven way to implement a comprehensive program. These frameworks provide guidance on how to organize your program, identify important capability gaps and measure capability maturity. Frameworks also provide a means to communicate program progress

to senior leaders within organizations that may not be well versed in cybersecurity tactics. Appropriately, President Obama directed the National Institute of Standards and Technology (NIST) to develop a security framework that could be used as a guide to secure the country's critical cyber infrastructure. This includes the development of an energy sector specific cybersecurity framework.

Our research identified just over half of respondents have adopted a cybersecurity framework of any kind, and only 11 percent have adopted the NIST cybersecurity framework. An additional 22 percent indicated that adopting the NIST framework is a future priority.

A New Approach Is Needed

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 our 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 resources on the highest priority risks.
- Organizing your organization's cybersecurity tactics using a programmatic framework.
- Building foundational capabilities and methodically maturing and improving them.
- Demonstrating tangible progress and performance.

Senior leaders need to be engaged in setting an enterprise cybersecurity vision. A programmatic framework to implement this vision and manage and improve its performance should be put in place. Organizations need to have confidence that they are directing their cybersecurity efforts and resources in a way that allows them to appropriately manage cyber risks.

Jon Kerner leads ScottMadden's cybersecurity practice and has helped a number of energy organizations improve the management and governance of their cybersecurity programs. He can be reached at *jkerner@scottmadden.com*.