White Paper

Utility and Energy Security: Responding to Evolving Threats

Utilities and energy organizations are part of the critical infrastructure of any nation, which makes them a high-profile target for cyberterrorists and hackers alike. Modernization brings gains in efficiency, but it also increases the attack surface through which threat agents can target utility infrastructure.

Utilities are under constant scrutiny from regulators to comply with IT security standards. Although regulations may contribute to a higher level of sophistication in the industry, they may also influence organizations to perceive compliance as being a sufficient investment in security. However, regulations may take a long time to incorporate changes. To be ahead of cyber attackers and respond to evolving threats, utilities must do more than simply comply with regulations.

Major Findings

In this paper, Cisco experts analyze the IT security capabilities of the utilities sector using data from the Cisco Security Capabilities Benchmark Study.[1] In our analysis we found that:

- Because utilities are heavily regulated and must take certain steps toward compliance, their IT security staff tend to view their organizations as attentive to security needs. In fact, this is the only industry in which the views of chief information security officers (CISOs) and security operations (SecOps) managers seem closely aligned. Seventy-four percent of the CISOs and 67 percent of SecOps managers in utility organizations classified were classifiedas having an upper-middle or high level of IT security sophistication, based on their responses to the survey.
- Seventy-three percent of IT security professionals at utilities say they've suffered a public security breach, compared with 55 percent in other industries. Utilities must report when they suffer a data breach, which could partially explain the higher figure. But this high number of public breaches also shows that this industry is vulnerable and that its comparatively higher sophistication still needs to be improved upon.
- Fifty-six percent of the IT security professionals in utilities say they use cloud-based web security, compared with 36 percent of the respondents in other industries. Utilities may be adopting cloud-based security more

[1] For more information on this study and the other white papers in this series, see the final sections of this document.

quickly than others as a response to the number of breaches they have experienced and the resulting public scrutiny and pressure to shore up their defenses.

- Sixty-four percent of CISOs and SecOps managers in the utilities sector say they make use of mobile security tools, compared with 50 percent of security professionals in other industries. Utilities' willingness to adopt mobile security solutions may reflect the high mobility of their workforce.
- Despite utilities being more sophisticated than other industries, the overall low number of security threat defenses is worrisome. It also suggests that the managerial perception of the organizations' sophistication may not match reality.

One important note: The study focused primarily on IT security capabilities, not on the state of operational technology (OT) security.

Managing Security in a Heavily Regulated Environment

The security landscape for utility organizations is tightly controlled. Several forces shape how they address IT security issues and how they allocate funds to invest in the IT security infrastructure. For example, utilities may not always be able to unilaterally make investments to increase IT security protections. They can decide how to use their resources and reprioritize investments internally, but they cannot easily transfer these costs to customers. First they must ask regulators for permission to raise prices, and such processes can be slow.

In addition, utilities operate under a microscope: Governments know that utilities may be targets of cyberterrorism and hacktivism attacks, and they fear the impact that such an attack would have to the economy and to national security. An interruption in service at a utility could have damaging repercussions for businesses and local residents. It could also cause other critical insfrastructure, such as transportation and water supplies, to fail.

The advent of "smart grid" technology and the Internet of Things introduces new challenges not only on the operational side, but also to IT. IT and OT are becoming more interconnected and reliant on one another, and combining their unique security challenges widens a utility's attack surface. OT security professionals at utilities should not avoid smart grid technologies, but they should understand the security needs that are associated with them. In this new environment, seasoned IT security professionals and purpose-built IoT security solutions can add value within the OT environment.

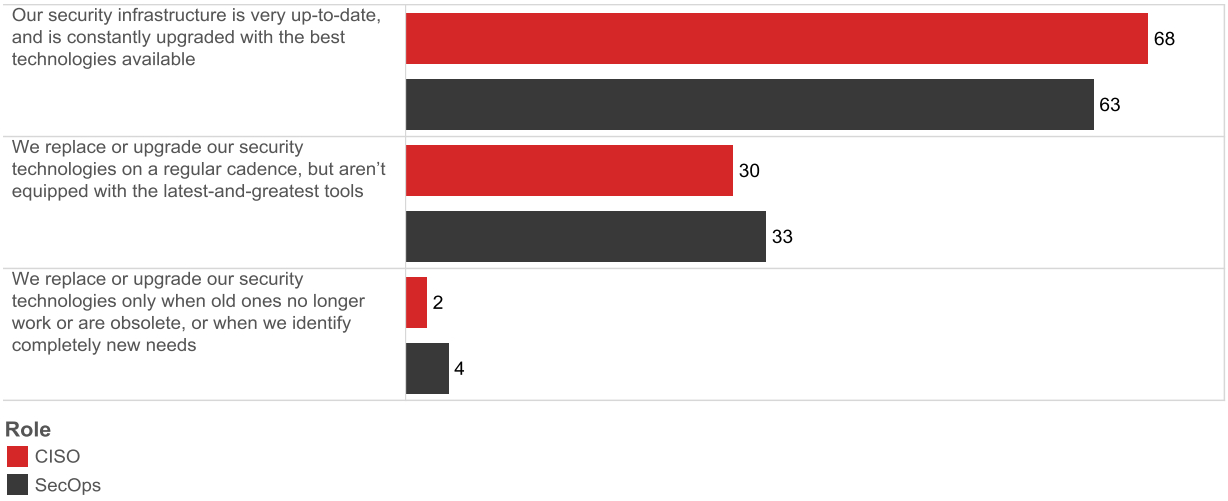
CISOs and SecOps Managers Aligned in Perceptions of Readiness

Utility CISOs and SecOps managers are relatively closely aligned in their view of their organizations' security sophistication, compared with those in other industries. Regarding their processes, 74 percent of CISOs categorized their organizations as having an upper-middle or high level of security sophistication (Figure 1). That was also the response of 67 percent of SecOps managers. This small gap in perception by CISOs and SecOps managers is unique to utilities. CISOs in other industries show significantly more optimism in IT security sophistication, processes, and tools than SecOps managers. In utilities, regulatory requirements, which define how organizations must manage data and respond to security incidents, appear to influence the opinions of both groups.

Figure 1. Perception of Organizational Security Sophistication, by Role

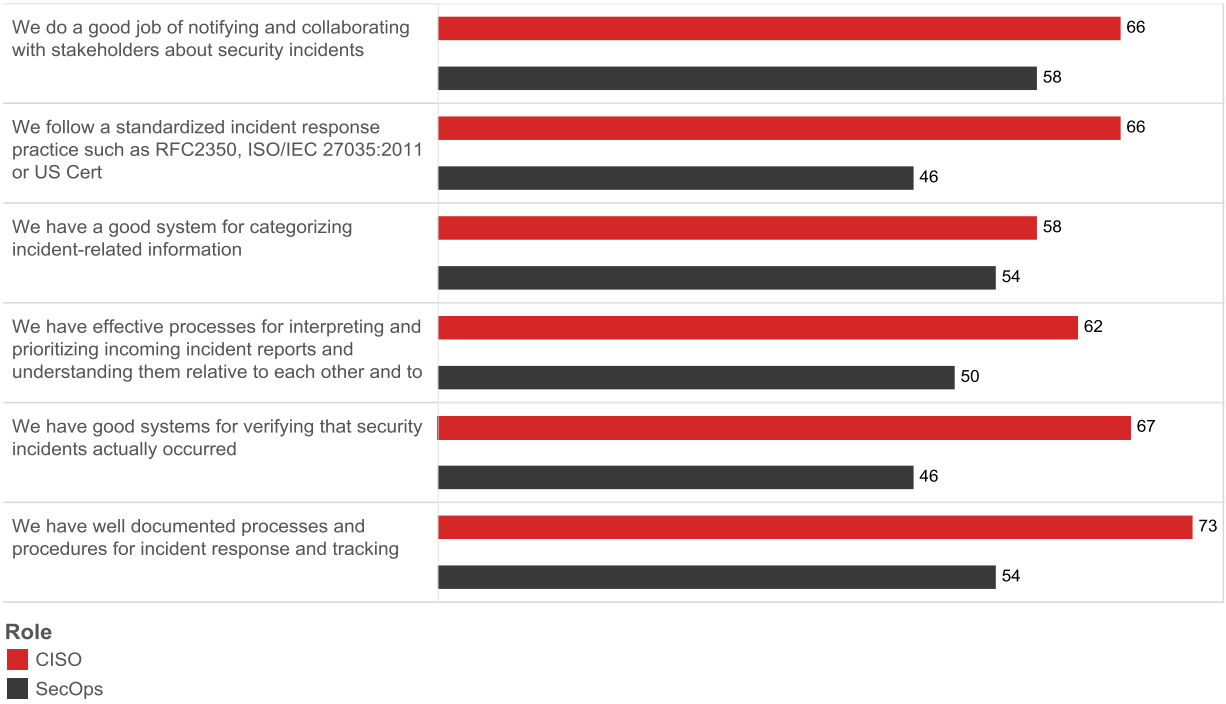
Likewise, CISOs and SecOps managers in utilities are more aligned than professionals in other industries when asked whether their IT security infrastructure is up to date. Sixty-eight percent of CISOs agreed that their infrastructure is continually upgraded with the best technologies available, and 63 percent of SecOps managers agreed. The perceptions of those who fall in the opposite camp were also in alignment. Thirty percent of CISOs say that they regularly replace technologies, but don't believe they are equipped with the latest tools, and 33 percent of SecOps managers say the same (Figure 2).

Figure 2. Similar Views Regarding Security Infrastructure (in Percentages)



Interestingly, the opinions of CISOs and SecOps managers diverge somewhat when the conversation turns to IT security controls. For example, 67 percent of CISOs say that their organizations have adequate systems for verifying that security incidents have actually occurred, but only 46 percent of SecOps managers say they have such systems in place (Figure 3). Also, 73 percent of CISOs say they have well-documented processes for incident response and tracking, while just 54 percent of SecOps managers say they have such systems.

Figure 3. Misalignment Regarding Security Controls (in Percentages)

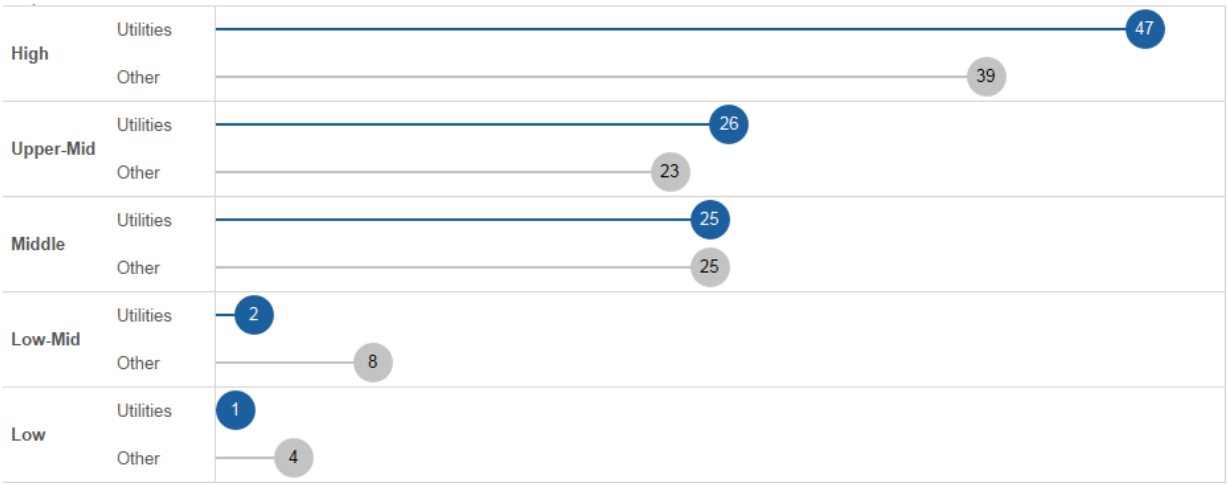


Management and technology structures in utilities are more complex than in many other industries. Therefore, even though the overall alignment between CISOs and SecOps managers is comparatively better, a lot of work still needs to be done to achieve a higher level of executive engagement and alignment across the entire organization. The importance of having well-defined processes and forensics capabilities cannot be overstated. Utilities need such capabilities to react quickly and identify root causes or anomalies when they occur.

Utilities More Sophisticated than Other Industries

Strong regulatory requirements—not to mention concerns about maintaining critical infrastructure—appear to raise the security technology sophistication of the utilities industry above that of other industries. Based on the responses from IT security professionals in utilities and energy, 74 percent of the organizations were categorized as having either upper-middle or high level of IT security sophistication. In other industries, 62 percent of the organizations were considered to be at these levels (Figure 4). However, utilities are one of the most targeted, and most publicly breached, sectors in any country. Their current level of sophistication, despite being higher than that of other industries, is still not high enough.

Figure 4. IT Professionals' Perceptions of Organizational IT Security Sophistication (in Percentages)



Utilities Differ in Adoption of Security Tools

We compared the security tools used by organizations in the utilities sector and in other industries. In some cases, utilities appear more likely to adopt tools that can provide more efficient and easily administered security protections. For example, utility CISOs and SecOps managers are more likely to use cloud-based versions of common security tools—such as vulnerability scanning and web security—than their counterparts in other industries. Fifty-six percent of the survey respondents in utilities say they use cloud-based web security, compared with 36 percent of respondents in other industries (Figure 5).

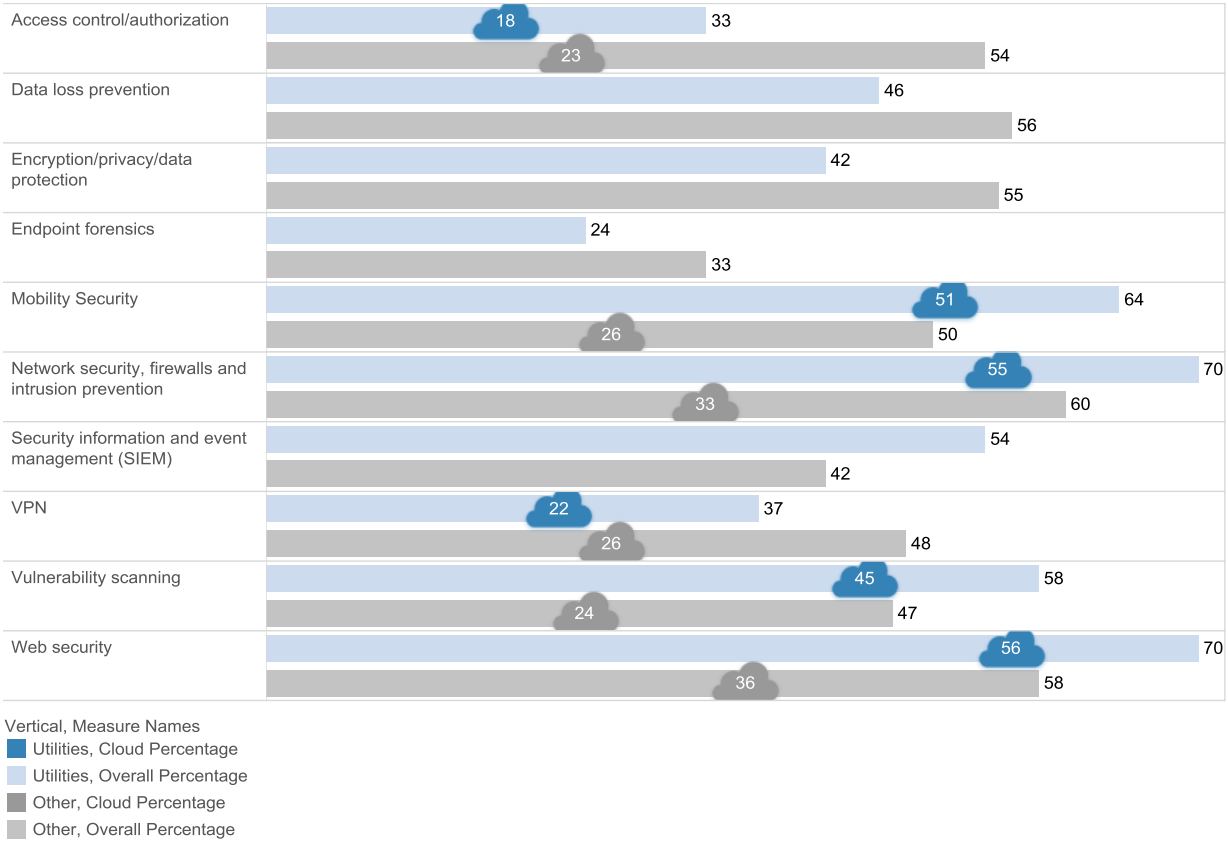
As for whether utilities are more likely to adopt threat defenses overall, regardless of platform, the answer depends on the tool in question. Seventy percent of security professionals in utilities say that they use network security, firewalls, and intrusion prevention systems, while 60 percent of security professionals in other industries use these tools. Sixty-four percent of utility CISOs and SecOps managers say they make use of mobile security tools, compared with 50 percent of security professionals in other industries (Figure 5).

Utilities' willingness to adopt mobile security solutions may reflect the high mobility of their workforce. Many employees are out in the field and need remote access to information—hence the greater focus on safeguarding mobile data.

CISOs and SecOps managers in utilities are less likely to use certain tools than their colleagues in other industries. Although 56 percent of security professionals in other industries say they use data loss prevention tools, only 46 percent of utility security professionals say they use them. Fifty-five percent of security professionals in other industries say they use encryption and privacy data protection tools, compared with just 42 percent of those in the utilities sector (Figure 5).

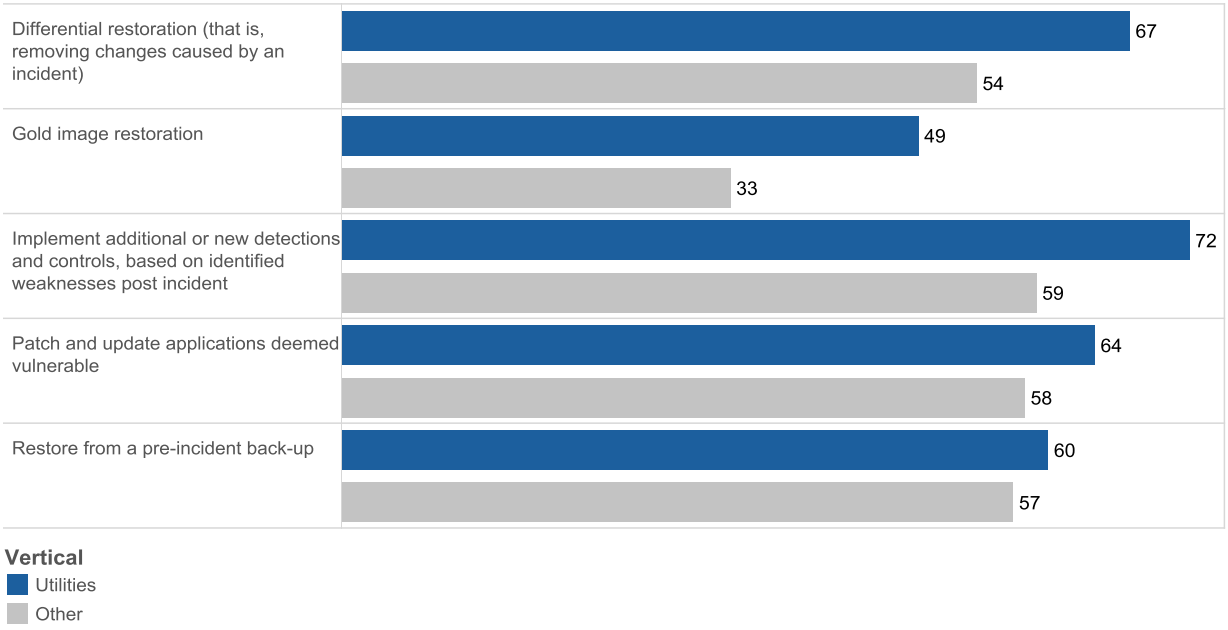
Despite utilities being more sophisticated than other industries, the overall low number of security threat defenses is worrisome. It also suggests that the managerial perception of their organizations' level of sophistication may not match reality.

Figure 5. Organizations Using Various On-Premises and Cloud-Based Security Threat Defenses (in Percentages)



After an incident, utilities are more likely to adopt tools to help restore the affected systems to their pre-incident levels. This response may be a result of their need to comply with regulations governing the industry. Utility security professionals say they use gold image restoration, differential restoration, and the patching of systems deemed vulnerable more often than professionals in other industries do (Figure 6).

Figure 6. Utilities Use More Processes to Restore Systems (in Percentages)



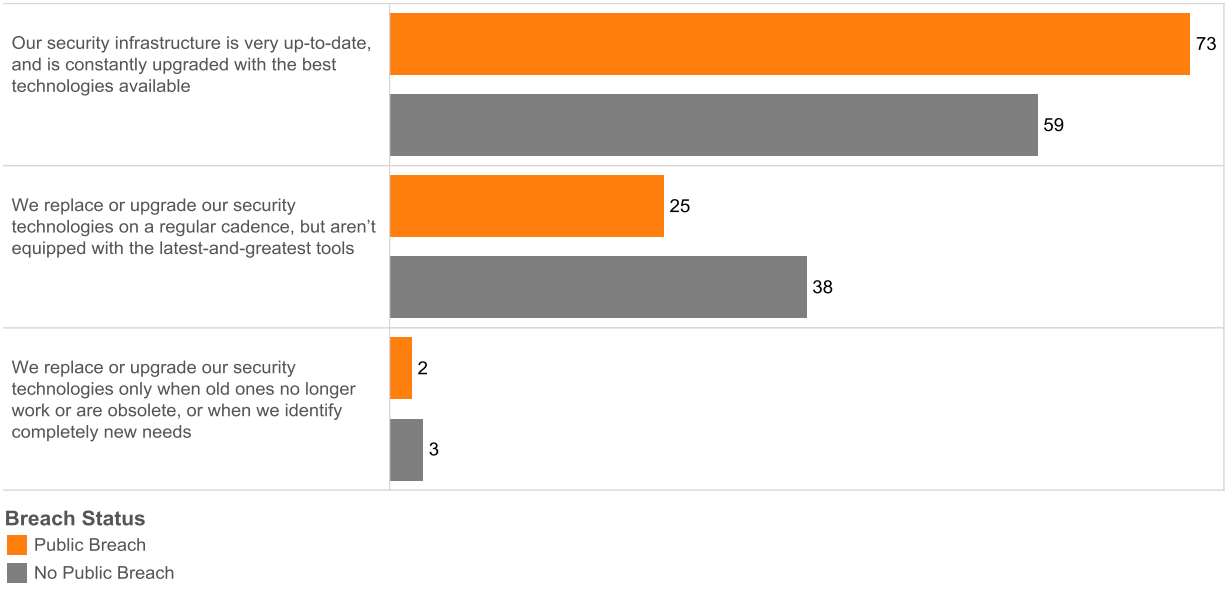
Utilities have to focus their investment on areas aligned with regulatory requirements. Expenditures in areas of security not yet covered by regulation can therefore be slow. Moreover, utilities cannot raise their prices to generate money for improvements, as a private company might do. The typical regulatory cycle for utility rate increases that are not an emergency may vary from three to six years.

Utilities More Likely to Experience a Public Security Breach

Utilities are frequently a target of cyber attacks because of their high public profile and the potentially damaging effects of a data breach or service disruption. In fact, 73 percent of utilities say they have suffered a security breach that led to public scrutiny, compared with 55 percent of other industries. This vulnerability further highlights the security challenges that utilities are facing. In many countries, utilities have to report breaches by law, a requirement that may have contributed to the high number of recorded breaches. Perhaps due to their tightly regulated environment, utilities are also slightly more likely than other industries to use internal security incident teams.

When they face public security breaches, utilities see these events as reality checks. Seventy-three percent of utilities that have not experienced a security breach that led to public scrutiny believe that their security infrastructure is up to date and constantly upgraded. Of the utilities that have experienced a public security breach, 59 percent believe their infrastructure is up to date (Figure 7).

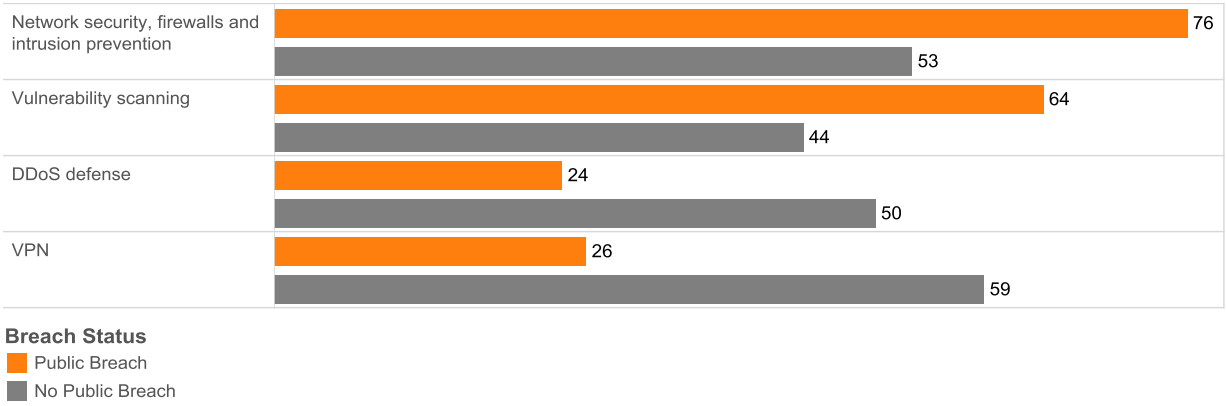
Figure 7. Security Breaches Change Readiness Perceptions (in Percentages)



Publicly breached utility companies lean more heavily on tools such as network security, firewalls, and intrusion prevention systems (IPS), instead of distributed denial-of-service (DDoS) defenses or VPN security tools. For example, 76 percent of utilities that have dealt with a public breach say they use firewalls and IPS tools, but only 53 percent of utilities that have not dealt with a public breach use them. Sixty-four percent of publicly breached utilities use vulnerability scanning tools, compared with 44 percent of non-publicly-breached utilities.

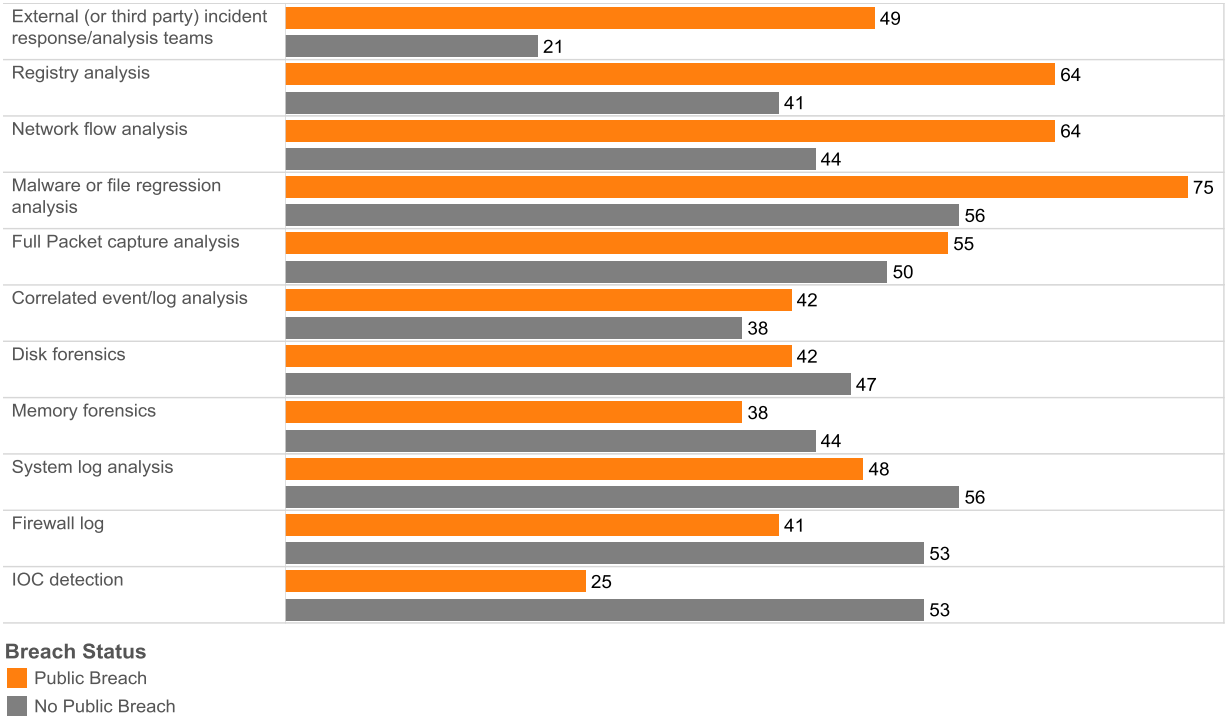
Conversely, 50 percent of non-publicly-breached utilities use anti-DDoS tools, compared with 24 percent of publicly breached utilities. And 59 percent of non-publicly-breached utilities use VPN security tools, while only 26 percent of publicly breached utilities do so (Figure 8).

Figure 8. Utilities' Use of Various Security Threat Defenses (in Percentages)



Public breaches appear to encourage utilities to more closely examine their security processes. For example, 64 percent of publicly breached utilities say they will quarantine or remove malicious applications. Only 41 percent of non-publicly-breached organizations say the same. Forty-nine percent of publicly breached organizations will use external incident response and analysis teams, while only 21 percent of non-publicly-breached utilities will do so (Figure 9).

Figure 9. Publicly Breached Organizations Adopt Tools to Analyze Compromised Systems (in Percentages)



Utilities that have experienced breaches that led to public scrutiny appear to also place a greater focus on strengthening security controls and restoring affected systems than their non-publicly-breached counterparts do. Seventy-eight percent of security professionals at publicly breached organizations say they have well-documented processes and procedures for incident response and tracking, compared with 50 percent of non-publicly-breached organizations.

Likewise, 63 percent of publicly breached organizations say they use gold image restoration to restore affected systems, while only 18 percent of non-publicly-breached organizations do so.

Avoiding disruption is a primary concern for utilities, so it seems logical that organizations that have been publicly breached will prioritize tools that focus on minimizing downtime and restoring affected systems.

Conclusion: Moving Beyond Regulatory Compliance

Utilities have to comply with many regulatory requirements. This need has influenced the security tools they use, their processes, their policies, and their budget priorities. It even affects the way CISOs and SecOps managers perceive their capabilities.

However, regulatory compliance can sometimes lead to utilities being overconfident in their IT security infrastructure. New technologies bring new challenges, and threats are evolving faster than regulators can develop new standards. Regulations should be considered a baseline, not an all-encompassing solution. Executives in this industry have to continue to invest their time and effort in understanding how the IT security landscape is changing. They must be quick to adapt, focusing on business objectives and understanding that cybersecurity is an ongoing process.

Utilities may seem better in its security practices than other industries. But they have suffered significantly more public breaches, which indicates that they still have to improve their existing capabilities.

Utilities should also consider how their investment in security from an IT perspective can support their operational technology (OT) and the continuous modernization and growth of their business. IT and OT convergence is becoming more frequent with smarter grids, and its success relies on strong cooperation between these two areas. This integration should extend to security.

Learn More

To learn how to become more resilient to new attacks and compete more safely in the digital age, get the Cisco 2016 Annual Security Report at www.cisco.com/go/asr2016.

To learn about Cisco's comprehensive advanced threat protection portfolio of products and solutions, visit www.cisco.com/go/security.

About the Cisco 2014 Security Capabilities Benchmark Study

The Cisco 2014 Security Capabilities Benchmark Study examines defenders across three dimensions: resources, capabilities, and sophistication. The study includes organizations across several industries, in nine countries.

In total, we surveyed more than 1700 security professionals, including chief information security officers (CISOs) and security operations (SecOps) managers. We surveyed professionals in the following countries: Australia, Brazil, China, Germany, India, Italy, Japan, the United Kingdom, and the United States. The countries were selected for their economic significance and geographic diversity.

To read findings from the broader Cisco Security Capabilities Benchmark Study referenced in this paper, get the Cisco 2015 Annual Security Report at www.cisco.com/go/asr2015.

The latest version of the study is now available in the Cisco 2016 Annual Security Report: www.cisco.com/go/asr2016.

About This White Paper Series

A team of industry and country experts at Cisco analyzed the Cisco 2014 Security Capabilities Benchmark Study. They offer insight on the security landscape in nine countries and six industries (financial services, government, healthcare, telecommunications, transportation, and utilities). The white papers in this series look at the level of maturity and sophistication of the survey respondents and identify the common elements that indicate higher levels

of security sophistication. This process helped contextualize the findings of the study and brought focus to the relevant topics for each industry and market.

About Cisco

Cisco delivers intelligent cybersecurity for the real world, providing one of the industry's most comprehensive advanced threat protection portfolios of solutions across the broadest set of attack vectors. Cisco's threat-centric and operationalized approach to security reduces complexity and fragmentation while providing superior visibility, consistent control, and advanced threat protection before, during, and after an attack.

Threat researchers from the Collective Security Intelligence (CSI) ecosystem bring together, under a single umbrella, the industry's leading threat intelligence, using telemetry obtained from the vast footprint of devices and sensors, public and private feeds, and the open source community at Cisco.

This intelligence amounts to a daily ingestion of billions of web requests and millions of emails, malware samples, and network intrusions. Our sophisticated infrastructure and systems consume this telemetry, enabling machine-learning systems and researchers to track threats across networks, data centers, endpoints, mobile devices, virtual systems, web, email, and from the cloud to identify root causes and scope outbreaks. The resulting intelligence is translated into real-time protections for our products and services offerings that are immediately delivered globally to Cisco customers.

The CSI ecosystem is composed of multiple groups with distinct charters: Talos, Security and Trust Organization, Active Threat Analytics, and Security Research and Operations.

To learn more about Cisco's threat-centric approach to security, visit www.cisco.com/go/security.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA 10/15