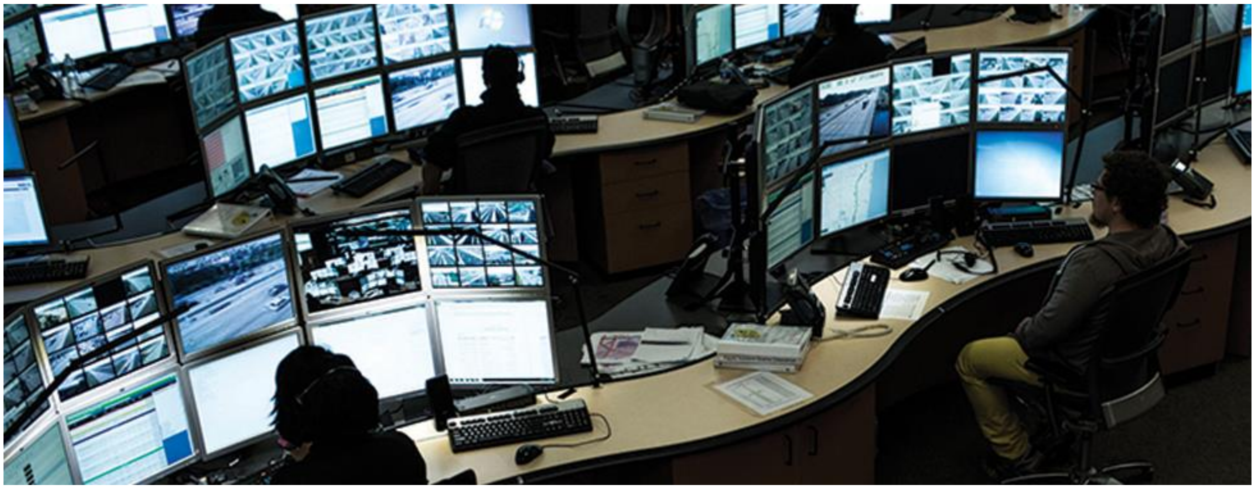
Security in Transportation: Preparing Defenses for a New Connected Era



Transportation is a complex ecosystem that is part of the critical infrastructure of any city, state, or nation. Any disruption to transportation networks—from roads to rail lines to waterways to the skies—can have an immediate and significant impact on citizens and the economy. Not surprisingly, the sector is a prime target for cybercriminals, hacktivists, and other bad actors.

- The Internet of Things (IoT) and its connected technologies, such as “smart” cars and highways, introduce even more opportunities for adversaries. They may exploit this connectivity to steal intellectual property, conduct espionage, and more. A lack of security can therefore limit the adoption of modern technologies. Conversely, strong security can enable growth in a connected era.
- Some organizations in this industry mistakenly believe that keeping older and less connected technology reduces their exposure to threats. They hold on to their proprietary systems. This posture may limit transformation in the sector. As threats continue to evolve quickly, these organizations may have to change the way they think about security.

Major Findings

In this paper, Cisco experts analyze the IT security capabilities of the transportation industry, using data from the Cisco 2014 Security Capabilities Benchmark Study.[1] In our analysis we found that:

- Transportation organizations use fewer security defenses overall than organizations in other industries. They are also less likely to use cloud-based defenses, probably in an attempt to reduce the risk of data exposure.

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

- Organizations in the industry also use fewer processes to analyze compromised systems, eliminate the causes of security incidents, and restore affected systems. The lack of security maturity, limited funds, and the low priority placed on security may be major factors for this trend.
- Publicly breached transportation organizations use fewer tools than non-publicly-breached organizations in the sector. However, more publicly breached organizations than non-publicly-breached organizations perceive the tools they have as being effective. These findings suggest that a public breach may help shift an organization's focus from simply owning solutions to applying them more effectively and improving the processes to support them.
- Transportation organizations with high levels of security sophistication typically have executives with well-defined roles and responsibilities around security. They also have well-documented procedures for incident response and tracking.

A New Era for Transportation

There is no question that technology can bring many benefits to transportation. Automated processes and intelligent controls can reduce delays and human error, preserve resources, improve connectivity, and provide a better customer experience.

As populations continue to grow, the pressure on the transportation sector increases. Transportation organizations have to operate more efficiently, and also more safely and securely. Technology such as the IoT is helping build the next generation of transportation. But it also widens the attack surface.

This concern has led to the misconception that using older and less connected technology reduces the exposure to threats. Many organizations hold on to proprietary systems, thinking it will help them avoid security risks. However, moving away from outdated technology can actually reduce vulnerabilities and simplify maintenance. Organizations can also build security into new systems from the outset.

Transitioning from an analog to a digital world requires a long-term commitment and investment. Technology upgrades can be challenging in transportation due to the complexity and expanse of the physical infrastructure. The industry also faces challenges such as a lack of funds for capital investments.

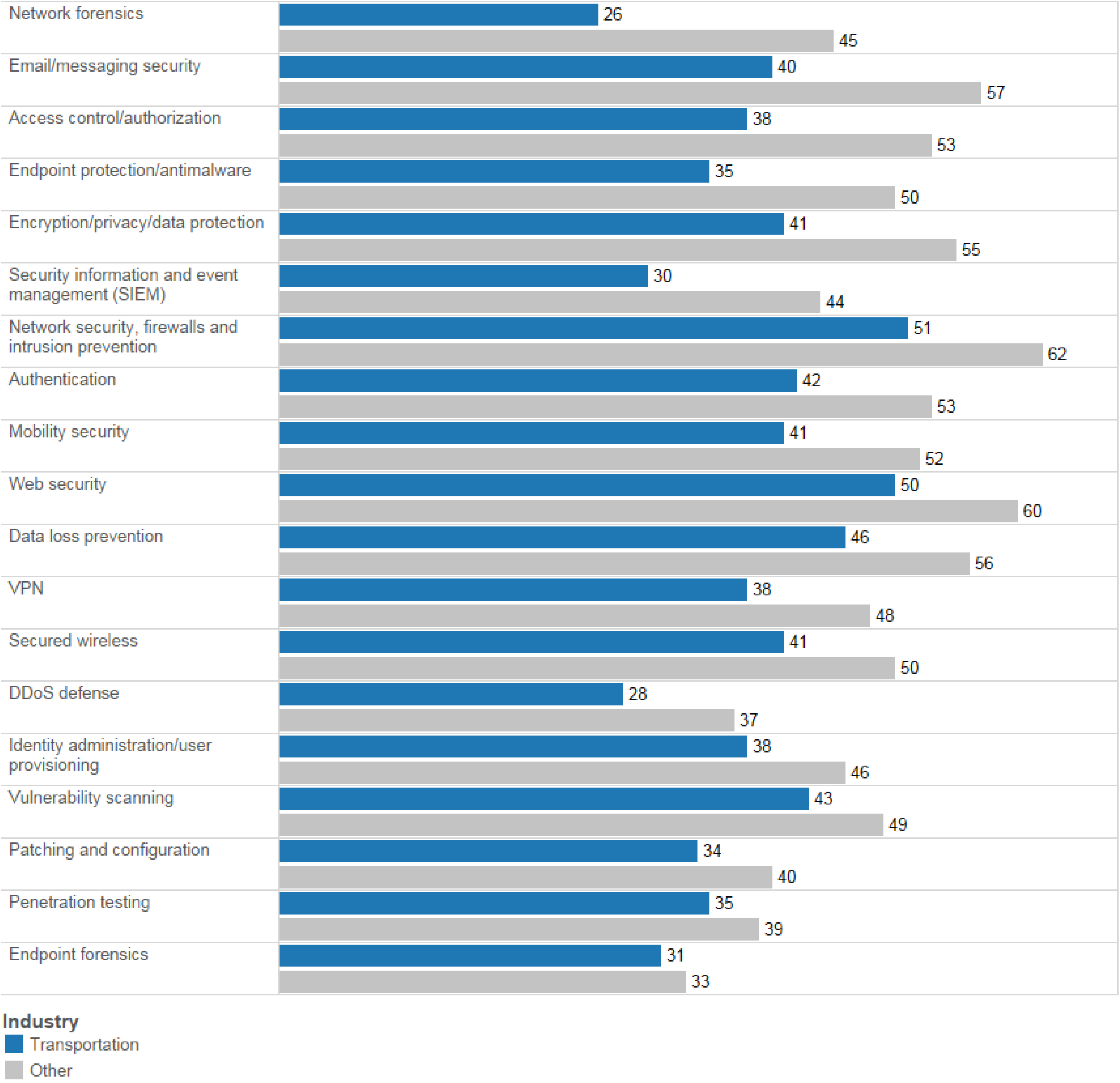
Many countries either already have or are drafting laws to protect their infrastructure. These legal requirements are likely to influence investments in technology. But they are not a complete solution for the security challenges in this industry. To keep up with evolving technologies and the changing security landscape, transportation organizations may have to rethink their security processes.

Transportation Industry Uses Fewer Defenses but Is Optimistic About Its Security Sophistication

Organizations in the transportation industry use fewer threat defenses than other industries do (Figure 1). Transportation seems to be missing some of the foundational tools not only for threat prevention but also for remediation. The industry lags behind other sectors in its adoption of defenses, both overall (Figure 1) and cloud-based (Figure 2), in five areas. These areas are:

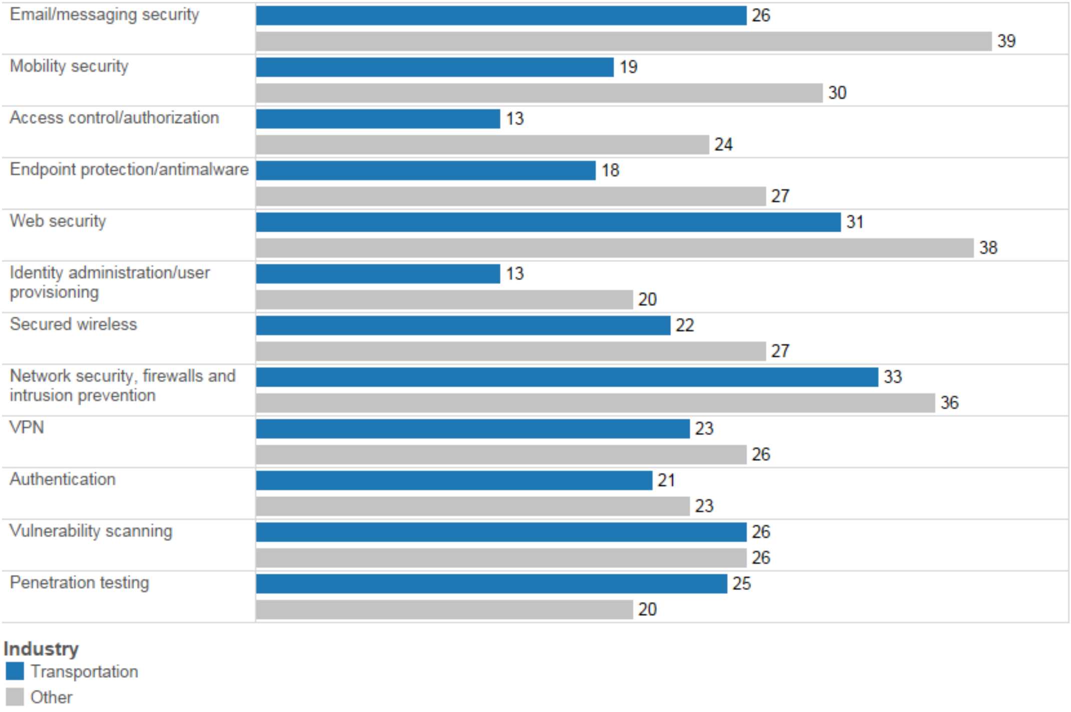
- Email and messaging security
- Mobility security
- Access control and authorization
- Identity administration
- User provisioning and network forensics

Figure 1. Percentages Organizations Using Various Threat Defenses



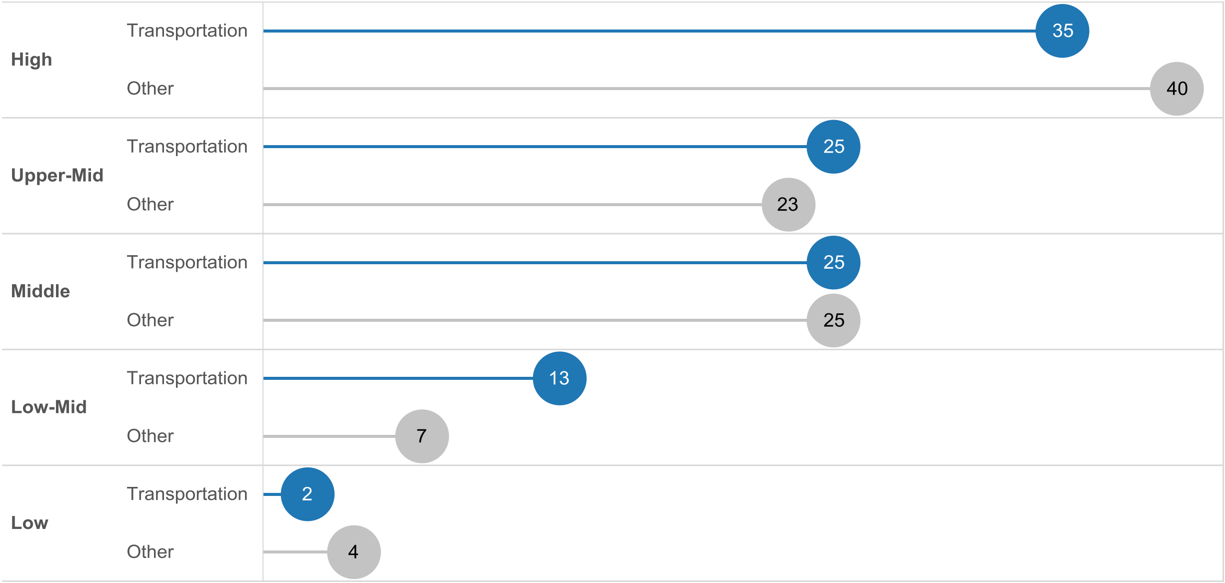
Transportation organizations may be avoiding cloud-based solutions because of their concern about data exposure. However, cloud-based solutions can offer flexibility and scalability. These benefits may be particularly valuable, given the expansion that this sector is going through and its limited resources for capital investments.

Figure 2. Percentages of Organizations Using Various Cloud-Based Threat Defenses



Surprisingly, the transportation organizations' lack of tools doesn't seem to negatively influence their security sophistication. In fact, this industry is on a par with other industries. Sixty percent of transportation organizations present either upper-middle or high levels of security sophistication. Sixty-four percent of organizations in other industries are at these same levels (Figure 3). This optimistic perception may be misguided.

Figure 3. Percentages of Organizations at Various Levels of Security Sophistication

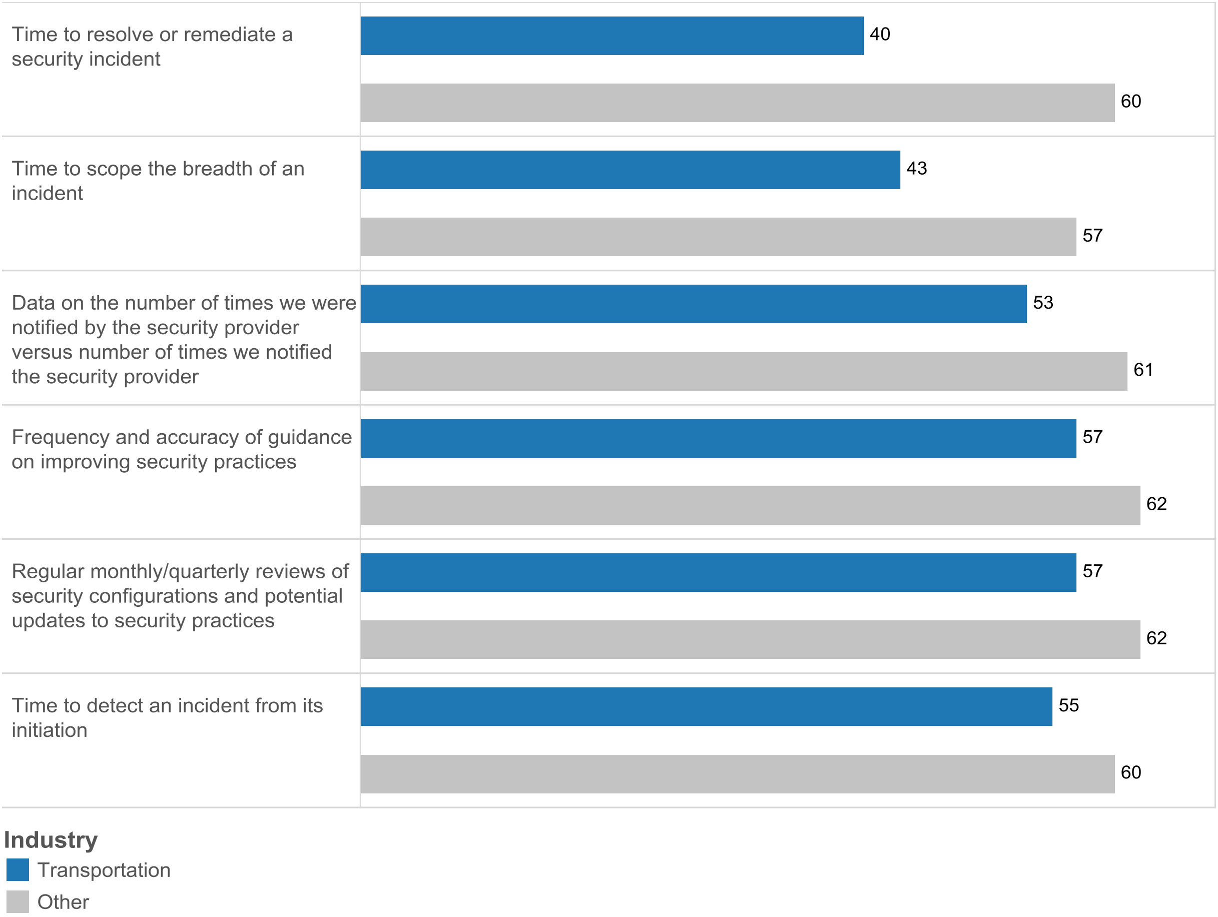


The transportation industry's use of third-party resources for security tasks is on a par with other industries. However, organizations in this sector are less likely to keep track of how these providers perform. This is particularly true with regard to the time it takes to resolve and remediate a security incident, as Figure 4 shows. Only 40 percent of transportation organizations use this performance measure, compared with 60 percent of businesses in other sectors.

It is likely that transportation organizations are simply more focused on blocking attacks. In addition, many may falsely assume that not being digitally connected helps protect them from threats that are intended to infiltrate and disrupt networks and data centers.

However, organizations need to find appropriate ways to measure the performance of both outsourced and internally-provided services. Otherwise they cannot assess the efficacy of their security programs. Organizations can measure the time to detection, the time to remediation, and the breadth of an incident, among other parameters. In this way they can determine whether the third-party monitoring service is providing the desired protection.

Figure 4. Percentages of Organizations That Measure How Third-Party Service Providers Carry Out Various Tasks



Majority of Transportation Organizations Have Suffered a Public Security Breach

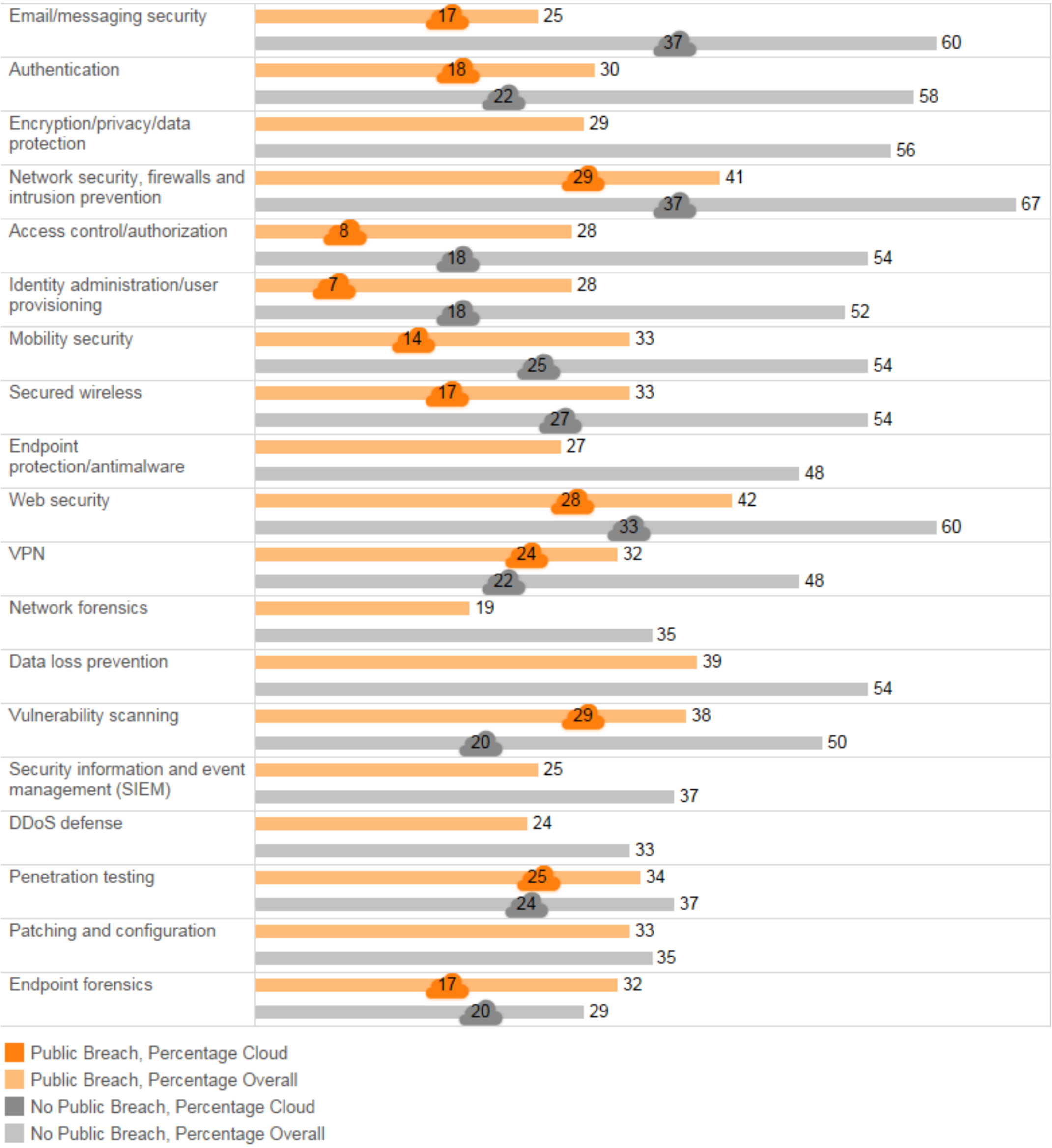
Sixty percent of transportation organizations have experienced a security breach that led to public scrutiny, compared with 56 percent in other industries. Transportation organizations are required by law in many countries to notify the authorities of any security incident that may lead to the failure or disruption of their services. In many cases these authorities withhold public disclosure if they believe the information will make citizens feel unsafe. It is surprising, therefore, that the percentage is still high.

Transportation organizations that have suffered a public security breach have weaker threat defenses in place, including cloud-based defenses, than organizations that have not suffered a public breach (Figure 5). Here again, network forensics emerges as an area where transportation organizations may want to improve. Although 35 percent of organizations that have not suffered a breach that led to public scrutiny report that they use network forensics, only 19 percent of organizations that have had a public breach use this defense measure (Figure 5). This tool is important for understanding the extent of a breach, the time it lasted, and the nature of any data stolen. Network forensics can thus assist executives when responding to public breaches. It can also provide intelligence that will help reinforce their organization's defenses in the future.

The gap between publicly breached and non-publicly-breached organizations is also accentuated in areas such as email and messaging security; authentication; network security, firewalls, and intrusion prevention; access control and authorization; and web security.

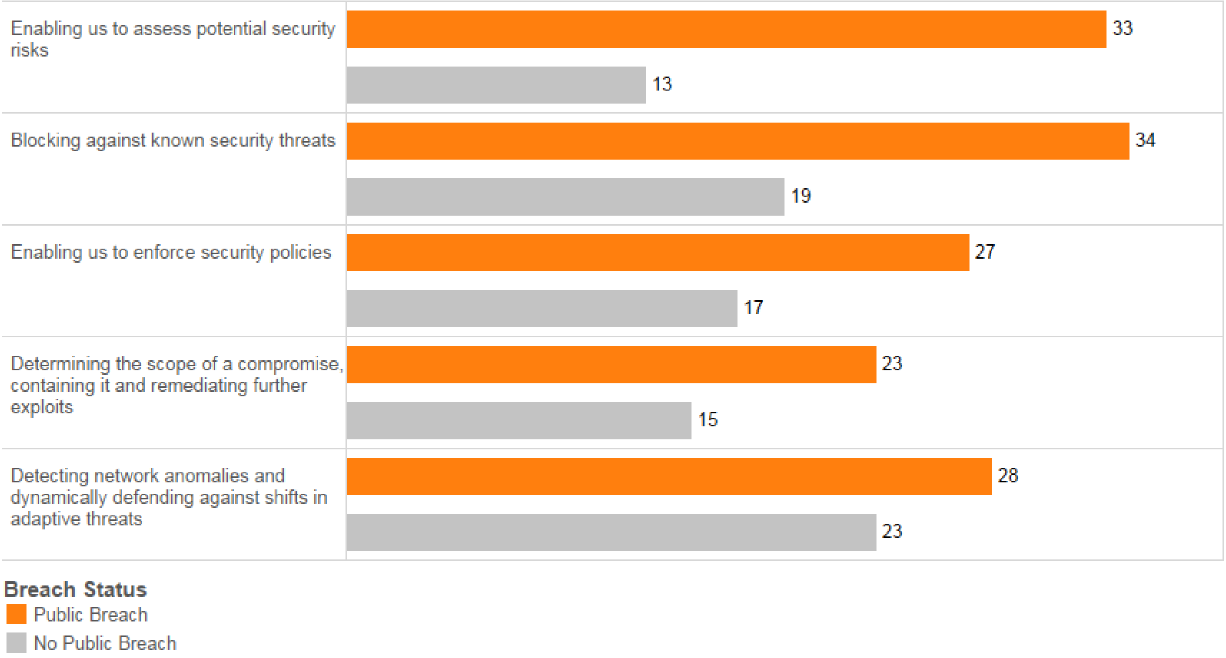
There are two potential explanations for these findings. Publicly breached organizations may in fact have weaker defenses than those that have not been publicly breached. But a public breach may change the organization's perception about the tools it has in place. It may also lead to higher self-criticism, especially about tools that are considered the first line of defense against threats.

Figure 5. Percentages of Transportation Organizations Using Various Threat Defenses, by Public Breach Status



On the other hand, transportation organizations that have suffered a public breach are more likely to report that their tools are extremely effective in enabling them to assess potential security risks (Figure 6). Changes that are implemented after a breach becomes public may explain this confidence.

Figure 6. Percent of Transportation Organizations That Perceive Tools to Be Extremely Effective in Various Functions, by Public Breach Status



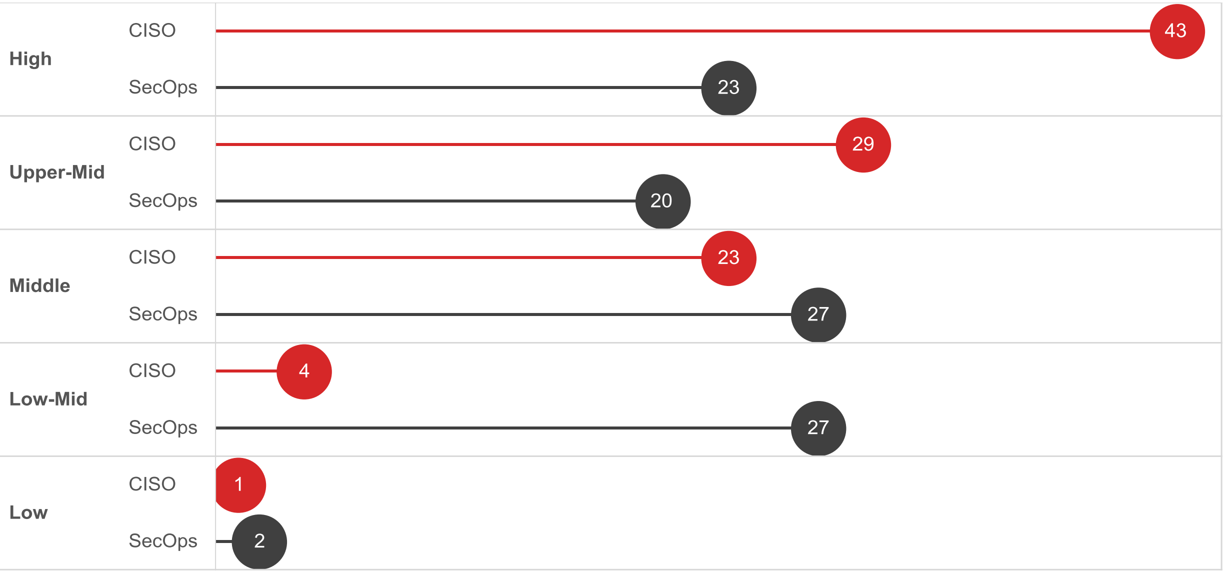
It is important to highlight that the overall numbers are low for both groups. At most, only a third of publicly breached companies perceive their tools as extremely effective. Among the non-publicly-breached organizations in this sector, the figures drop to below one-quarter.

CISOs and SecOps: A Significant Lack of Alignment in Perception of Security Sophistication

Chief information security officers (CISOs) and security operations (SecOps) managers working at transportation organizations are not aligned in their perceptions about their organization's level of security sophistication. CISOs are far more optimistic in their outlook: 72 percent of these security professionals were mapped as either "upper middle" or "high" in their perceptions of security sophistication, compared with 43 percent of SecOps managers (Figure 7).

This gap may be partly due to a blurring of the lines between traditionally assigned responsibilities. These roles may now need to be refined to close gaps and reduce overlaps. In addition, organizations may have to adopt new processes to allow tighter collaboration between the professionals in these roles.

Figure 7. Percentages of Transportation Organizations at Various Levels of Security Sophistication, Based on Perceptions of Their CISOs and SecOps Managers



In our overall study, there seems to be a gap in the security perceptions of CISOs and SecOps managers in nearly every industry and country. We attribute this lack of alignment largely to the fact that CISOs focus on the overall security strategy for the organization, while SecOps managers deal directly with the day-to-day “firefighting” of threats. A general lack of communication between these two groups, which is typical across industries, may exacerbate the difference. The closer that CISOs and SecOps managers work, the smaller the gap in their perceptions—and potentially the more realistic the outlook of the organization’s state of security.

Recommendations for Improving Security Sophistication

Transportation organizations that want to improve their overall security sophistication should take note of two particular characteristics of higher levels of maturity in this industry:

- The majority (80 percent) of security personnel in highly sophisticated organizations strongly agree that security roles and responsibilities are clarified within the executive team. Only half of the less sophisticated organizations strongly agree.
- In addition, 80 percent of the security personnel in these organizations strongly agree that they have well-documented processes and procedures for incident response and tracking, opposed to only 39 percent of the less sophisticated organizations.

Regardless of budget constraints, transportation organizations can make important strides in improving their security sophistication. They can emulate the key characteristics of their more mature counterparts by:

- Embracing digitization and recognizing that security can be an enabler of business growth.
- Being more proactive about assessing and mitigating security risks and implementing security plans. This includes recognizing that fast-emerging technologies—from autonomous vehicles to automated traffic control systems to drones—are creating both new opportunities and new risks for the transportation industry.

- Assuming that breaches will most likely happen. They can then build a plan to identify, mitigate, and remediate these threats before they can create serious damage. Experiencing a public breach should not be the call to action for the organization to strengthen its security defenses.

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 global 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 11/15