Transportation: Improving Cybersecurity to Protect Emerging Systems

As populations grow, so does the need for transportation. Handling a growing number of passengers is not the only concern of transportation agencies. They need to continually improve safety, efficiency, reliability, and the customer experience. Technology may bring the answer to many of these modern issues, but it also brings challenges.

Cybercriminals are becoming more professional and creative about their methods. They look at connected vehicles and see an opportunity for hacking into a system.[1] Public transport such as airplanes or trains may also become targets.[2] An attacker can even hack into a cargo company to change a manifest and facilitate smuggling, drug trafficking, and other criminal activities.[3]

Connectivity is an irreversible trend. Transportation organizations should embrace it and focus on strengthening their security to enable next-generation systems. Specifically, they should:

- Think beyond the network perimeter. For example, a breach anywhere in one of their suppliers can affect the entire supply chain. Improving security throughout the industry will help the next generation of transportation be successful.
- Move faster to strengthen security and never stop evolving defenses, because adversaries innovate continuously and rapidly.

Major Findings

In this paper, Cisco subject-matter experts analyze the IT security capabilities of organizations in the transportation industry using comparative data from the Cisco 2015 Security Capabilities Benchmark Study.[4] For example, we learned that:

- Compared with other industries in our study, including utilities and energy, transportation has a greater percentage of organizations classified as highly mature in terms of their security sophistication. Most transportation companies reported having strong security processes and highly effective security tools.
- Compatibility issues with legacy systems and budget constraints are the top two obstacles to the adoption of security processes and technology.
- The vast majority of transportation organizations (92 percent) have an executive directly accountable for security, but only 61 percent of our respondents strongly agreed that their executive leadership considers security a high priority.
- More than 90 percent of the transportation organizations that endured public scrutiny following a data breach reported that the experience led to substantial security improvements.

Other Industries Can Provide Models for the Transportation Sector

As the transportation industry builds and expands next-generation systems, the organizations within it have an opportunity to help their sector succeed by securing every connection from device to application. New and emerging business models–such as on-demand freight shipping services–will further complicate and increase the need for security throughout the sector.

Many transportation companies hesitate to become more connected. They should look to industries such as financial services for insight. Security concerns initially prevented many financial institutions from embracing connectivity. However, they soon realized they were missing out on business benefits such as greater efficiency. They were also at risk of losing a growing population of customers who demand connectivity. So they began to think about how to increase connectivity securely, instead of avoiding it altogether.

Many financial institutions are improving their security architecture and addressing the gaps that traditional solutions cannot fill. Transportation organizations should consider a similar approach from the outset as they digitize and adapt to the Internet of Things (IoT). However, the organizations included in our study cited a number of obstacles standing in the way of adopting security processes and technology. These hurdles to improvement include compatibility issues with legacy systems and budget constraints (Figure 1). For comparison, Figure 1 also lists the obstacles faced by the utilities and energy industry.

---

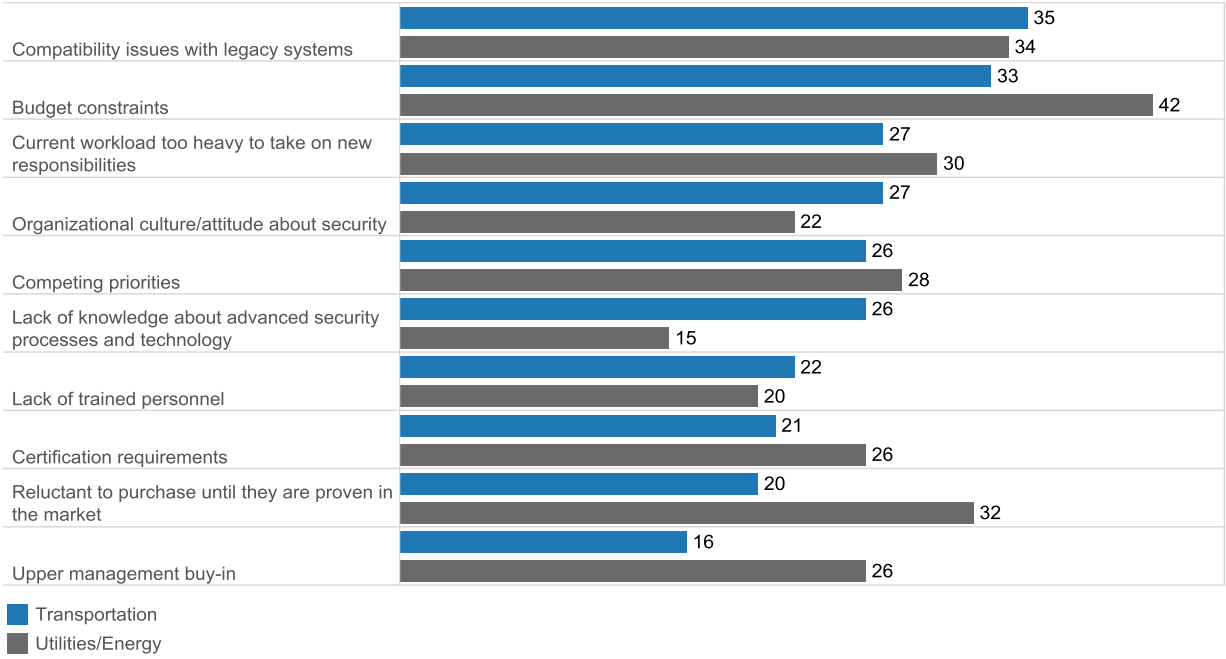
[1] "Hackers Remotely Kill a Jeep on the Highway–with Me in It, Wired, July 2015: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[2] "FBI: Hacker claimed to have taken over flight's engine controls," CNN, May 2015: http://edition.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/.

[3] "Police warning after drug traffickers' cyber-attack," BBC, October 2013: http://www.bbc.co.uk/news/world-europe-24539417

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

Figure 1. Top Obstacles to Adopting Security Processes and Technology: Transportation and Utilities/Energy, by Percentage



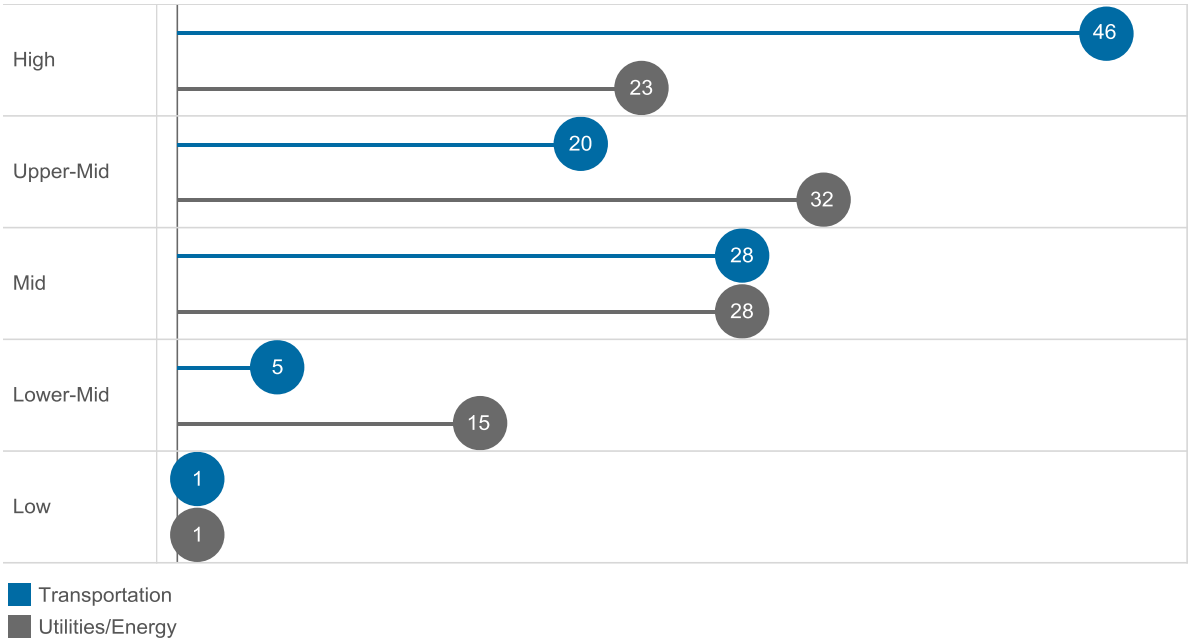
The IoT is increasing the need to digitize transportation applications. Many disparate proprietary systems must converge onto a single IP network to enable information sharing and common communications. This convergence will help transportation agencies create safer, more mobile, and more efficient operations. However, these agencies must keep IT security at the forefront of this undertaking.

Signs of Growing Security Sophistication

Many transportation organizations find it challenging to adapt security processes and technology as their industry transforms. But there are some positive indicators that the industry is on the right track.

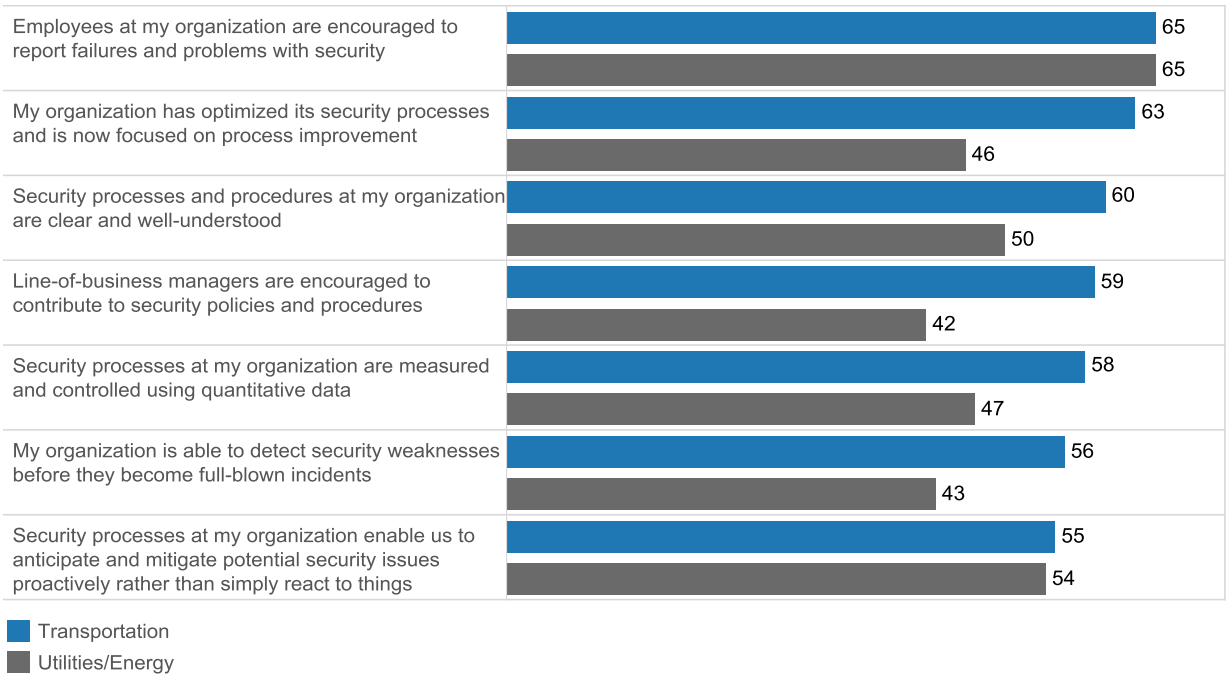
As seen in Figure 2, transportation has a greater percentage of highly mature organizations in terms of security sophistication (46 percent) than does the utilities and energy industry (23 percent).

Figure 2. Levels of Security Maturity in the Transportation and Utilities/Energy Industries, by Percentage



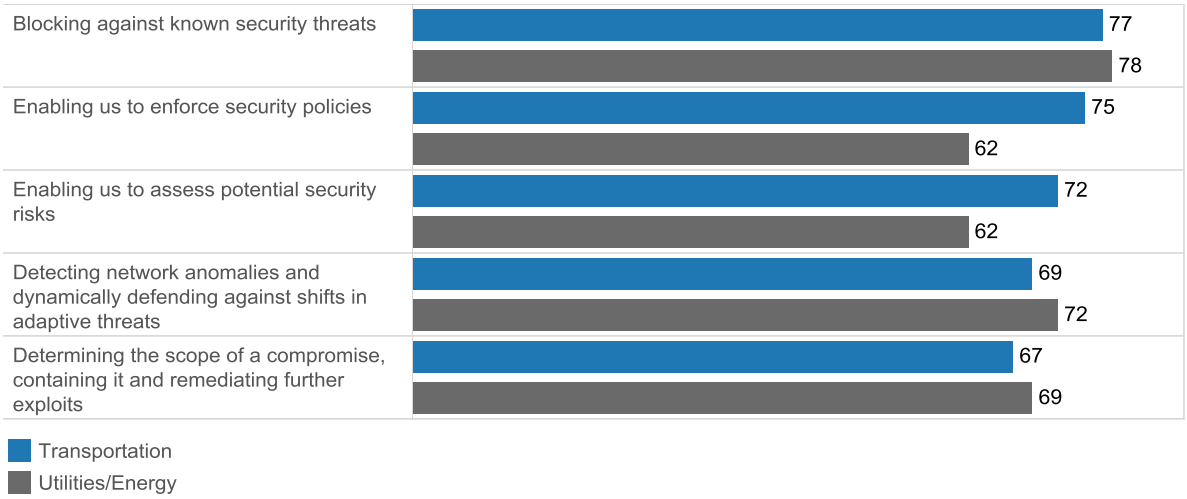
Organizations in the transportation sector strongly believe that they have optimized security processes and are now focused on improvement (Figure 3). Sixty-three percent of organizations in the industry described their security culture this way. As a point of comparison, less than half (46 percent) of respondents from the utilities and energy industry made the same assessment.

Figure 3. Views on Status of Security Culture: Transportation and Utilities/Energy (by Percentage)



Most organizations in transportation also expressed confidence in the effectiveness of their security tools. For example, 77 percent reported that their tools are highly effective at blocking known security threats (Figure 4.)

Figure 4. Percentages of Organizations Rating Their Security Tools as Highly Effective in Various Areas



The above findings suggest most transportation organizations are approaching a high level of security sophistication and are using effective security processes and tools. However, another data point indicates that many may need to confirm that their executive leadership is focused on improving security.

Ninety-two percent of transportation organizations said that they have an executive directly accountable for security. A similarly high percentage of businesses in other industries reported the same practice. However, just 61 percent of respondents in transportation organizations strongly agreed that their executive leadership considers security to be a high priority (Figure 5).

Figure 5. Percentages of Respondents Strongly Agreeing with Various Statements About Executive Leadership: Transportation and Utilities/Energy

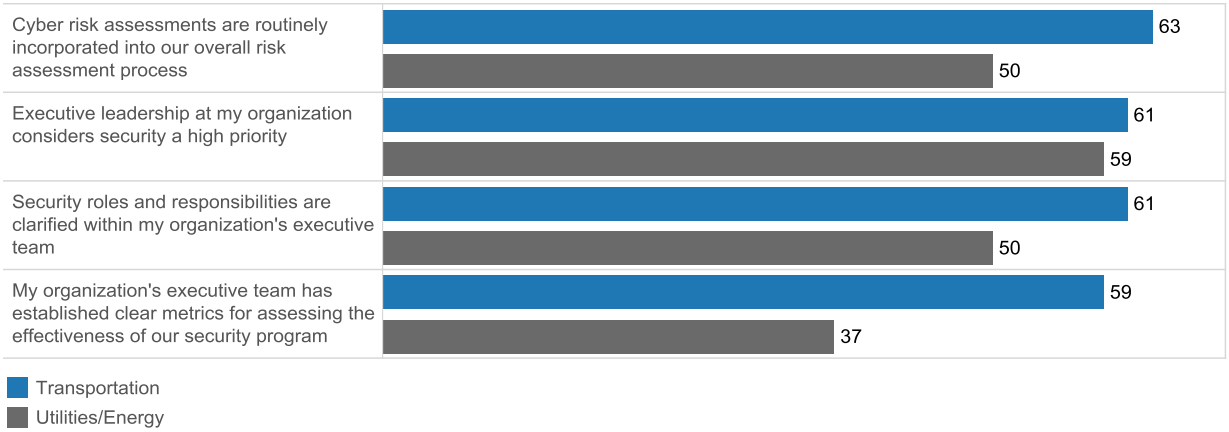


Figure 5 also highlights another stark contrast between the transportation industry and the utilities and energy sector. Fifty-nine percent of transportation organizations agreed that their executive team has established clear metrics for assessing the effectiveness of their organization's security program. Only 37 percent of utilities and energy businesses made the same statement.

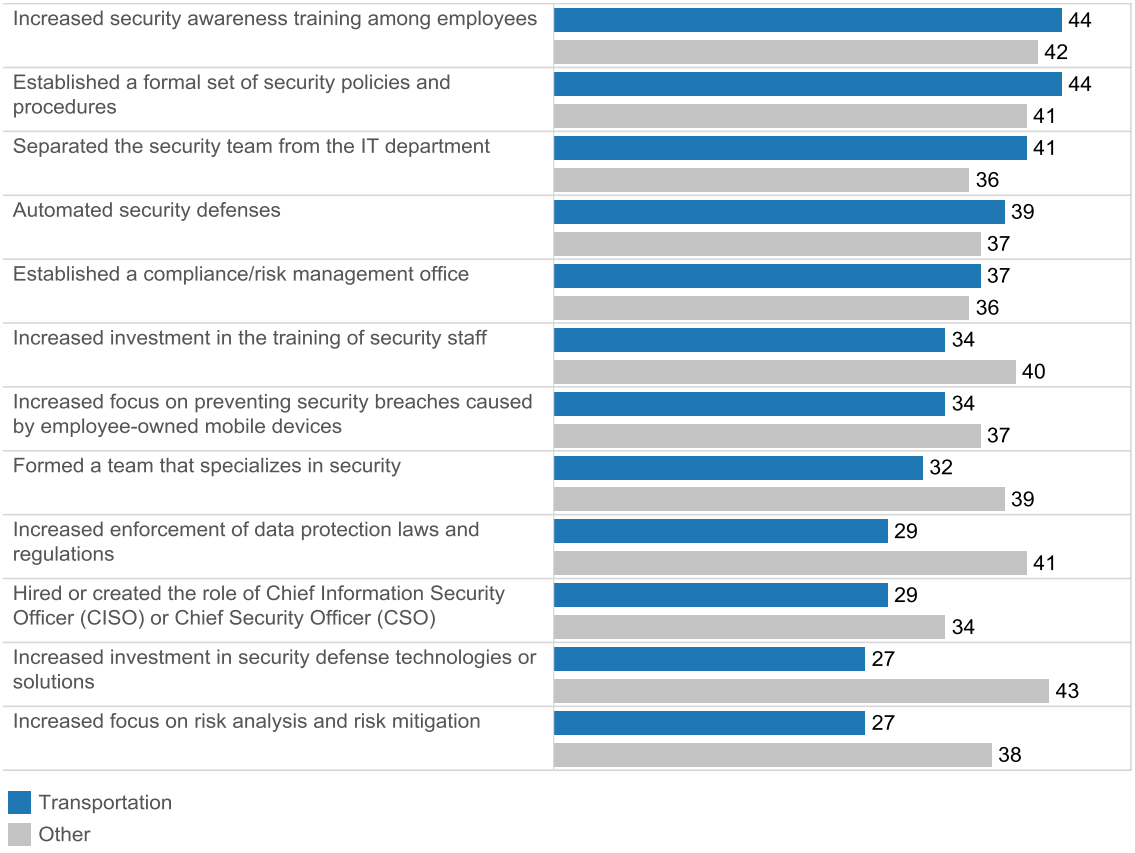
Public Scrutiny Following a Breach Leads to Security Improvement

About one-third (35 percent) of the respondents in transportation said they had suffered a security breach that led to public scrutiny. This is a significantly lower percentage than reported by other industries (49 percent).

Of the organizations in transportation that had endured public scrutiny following a breach, over 90 percent said the experience had led to substantial security improvements in their organization.

As Figure 6 shows, the top three improvements they have made include increasing security awareness training among employees (44 percent); establishing a formal set of security policies and procedures (44 percent); and separating the security team from the IT department (41 percent).

Figure 6. Types of Security Improvements Made Following a Public Breach: Transportation and Other Industries, by Percentage



These improvements are likely to benefit many transportation organizations in the long term. As the industry becomes a more likely target for cyber attacks, organizations will need to have dedicated teams focused on deterring, detecting, responding to, and remediating threats. For that reason, transportation organizations should explore the value of establishing a dedicated security operation center (SOC).[5]

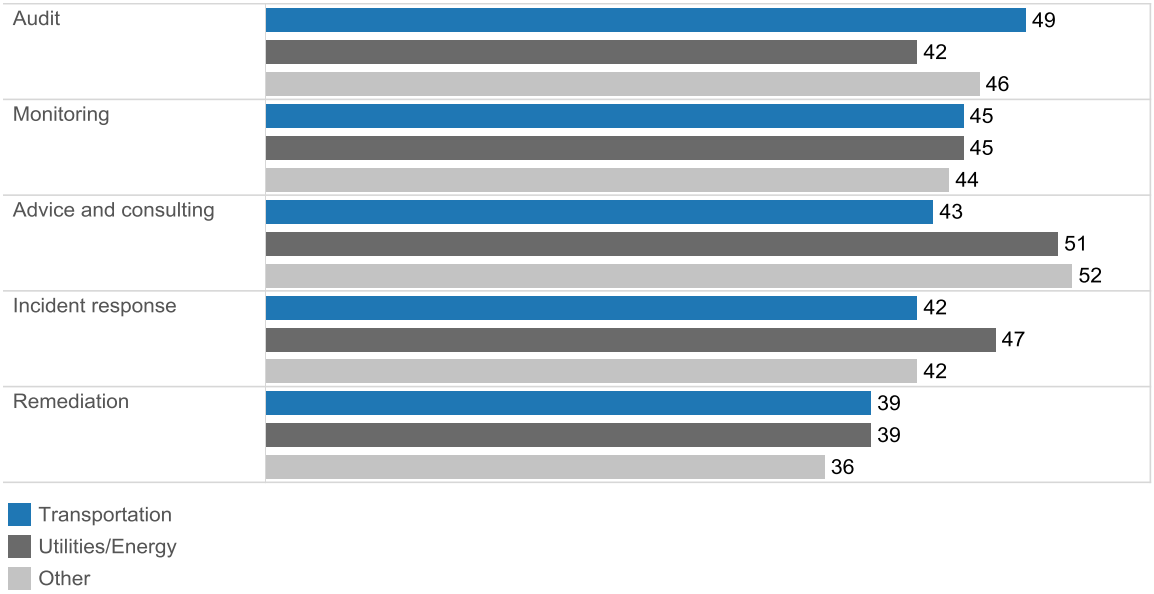
Another area for improvement is increasing investment in security defense technologies or solutions. As Figure 6 showed, only 27 percent of publicly breached transportation organizations increased their investments.

[5] A SOC is a centralized unit that deals with security issues on an organizational and technical level. For more information about SOCs, read this article: http://www.rsaconference.com/blogs/security-operations-center-building-operating-and-maintaining-your-soc

Most Transportation Organizations Outsource Security Tasks

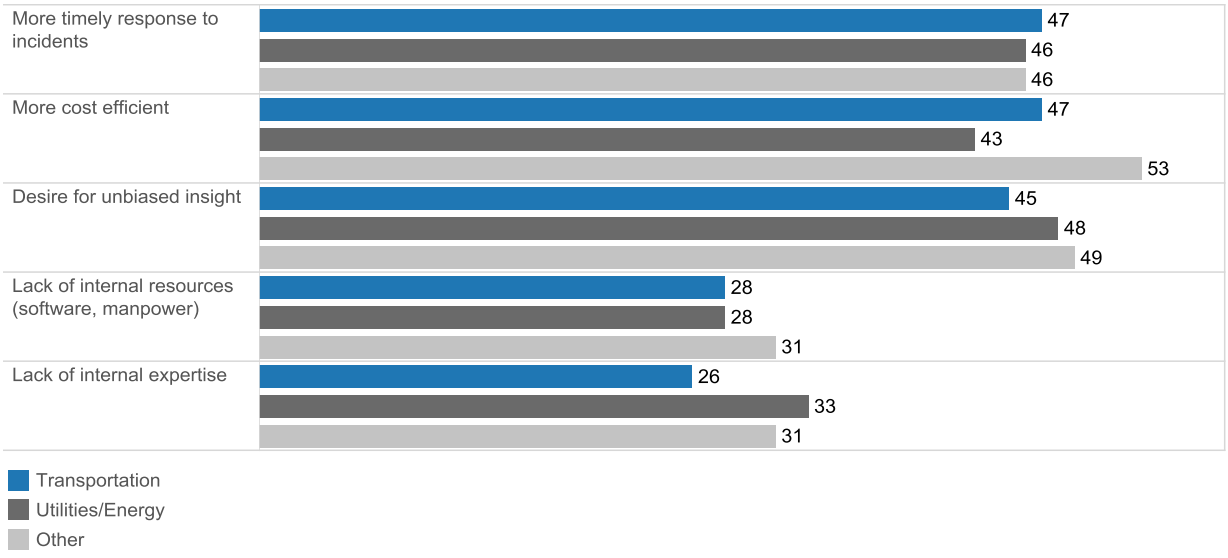
Most transportation companies (87 percent) rely on third-party experts to provide various security services either fully or in part. Forty-nine percent said they outsource IT auditing—more than any other industry in our study (see Figure 7). A similar percentage (45 percent) outsource security monitoring.

Figure 7. Percentage of Organizations Outsourcing Various Services Fully or in Part to External Parties, by Industry



Transportation agencies cited cost efficiency and the ability to respond to security incidents more quickly as the top two reasons for outsourcing (Figure 8). Few organizations in the industry said they engaged third parties to compensate for a lack of internal resources or expertise.

Figure 8. Reasons Why Industries Outsource Security Services, by Percentage



Conclusion: The Time Is Now to Prepare Defenses

The transportation industry appears to be on the right track with improving its security sophistication. It is imperative that organizations in the sector continue building on this momentum. More than that, they should work to advance their security sophistication even further, as quickly as possible. This will allow them to meet new cybersecurity challenges as systems become more autonomous and connected and new business models emerge.

Cybercriminals, hacktivists, and other threat actors will seek to exploit vulnerabilities in an increasingly connected environment. As the IoT continues to expand, organizations in the sector must realize that connectivity and digital transformation are inevitable, well under way, and irreversible. These organizations should take steps now to:

- Ensure that executive leadership makes cybersecurity investment a high priority and part of the organization's formal capital plan
- Develop an integrated security architecture to cover gaps that point solutions cannot address, especially as the organization becomes more connected
- Understand the threat landscape and monitor how it evolves

Recognizing that the transportation industry is a prime target for attacks, and knowing what and where the risks are, are imperative to making security improvements that will protect transportation systems, agencies, and users.

Organizations also need to build an integrated security architecture and consider starting up a SOC, if they have not done so already. In fact, the industry as a whole should strive to create an integrated security architecture and improve the sharing of information and best practices. Information sharing and analysis centers (ISACs),[6] for example, are likely to prove valuable to all organizations in the sector as transportation undergoes a digital transformation to become more autonomous and connected.

Learn More

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

About the Cisco 2015 Security Capabilities Benchmark Study

The Cisco 2015 Security Capabilities Benchmark Study examines defenders across three dimensions: resources, capabilities, and sophistication. The study includes organizations across several industries in 12 countries. In total, we surveyed more than 2400 security professionals, including chief information security officers (CISOs) and security operations (SecOps) managers. We surveyed professionals in the following countries: Australia, Brazil, China, France, Germany, India, Italy, Japan, Mexico, Russia, the United Kingdom, and the United States. The countries in the survey were selected for their economic significance and geographic diversity.

To read findings from the broader Cisco Security Capabilities Benchmark Study, get the Cisco 2016 Annual Security Report at www.cisco.com/go/asr2016.

About This Series

A team of industry and country experts at Cisco analyzed the Cisco 2015 Security Capabilities Benchmark Study. They offer focused insight on the security landscape in 10 countries and four industries (financial services, healthcare, telecommunications, and transportation). The white papers in this series highlight the security

[6] An ISAC is a nonprofit organization that provides a central resource for gathering information on cyber attacks to critical infrastructure and providing two-way sharing of information between the private and public sector. For an example, see the Surface Transportation Information Sharing & Analysis Center website: https://www.surfacetransportationisac.org/.

landscape and challenges that organizations face in cybersecurity. This process helped to contextualize the findings of the study and bring focus to the relevant topics for each country and industry we analyzed.

About Cisco

Cisco is building truly effective security solutions that are integrated, automated, open and simple to use. Drawing on unparalleled network presence as well as the industry's broadest and deepest technology and talent, Cisco delivers ultimate visibility and responsiveness to detect more threats and remediate them faster. By calling on Cisco Security, companies are poised to securely take advantage of a new world of digital business opportunities.

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.**