1-2019

Managing Cyber Risks & Business Exposure in the Surface Transportation Ecosystem

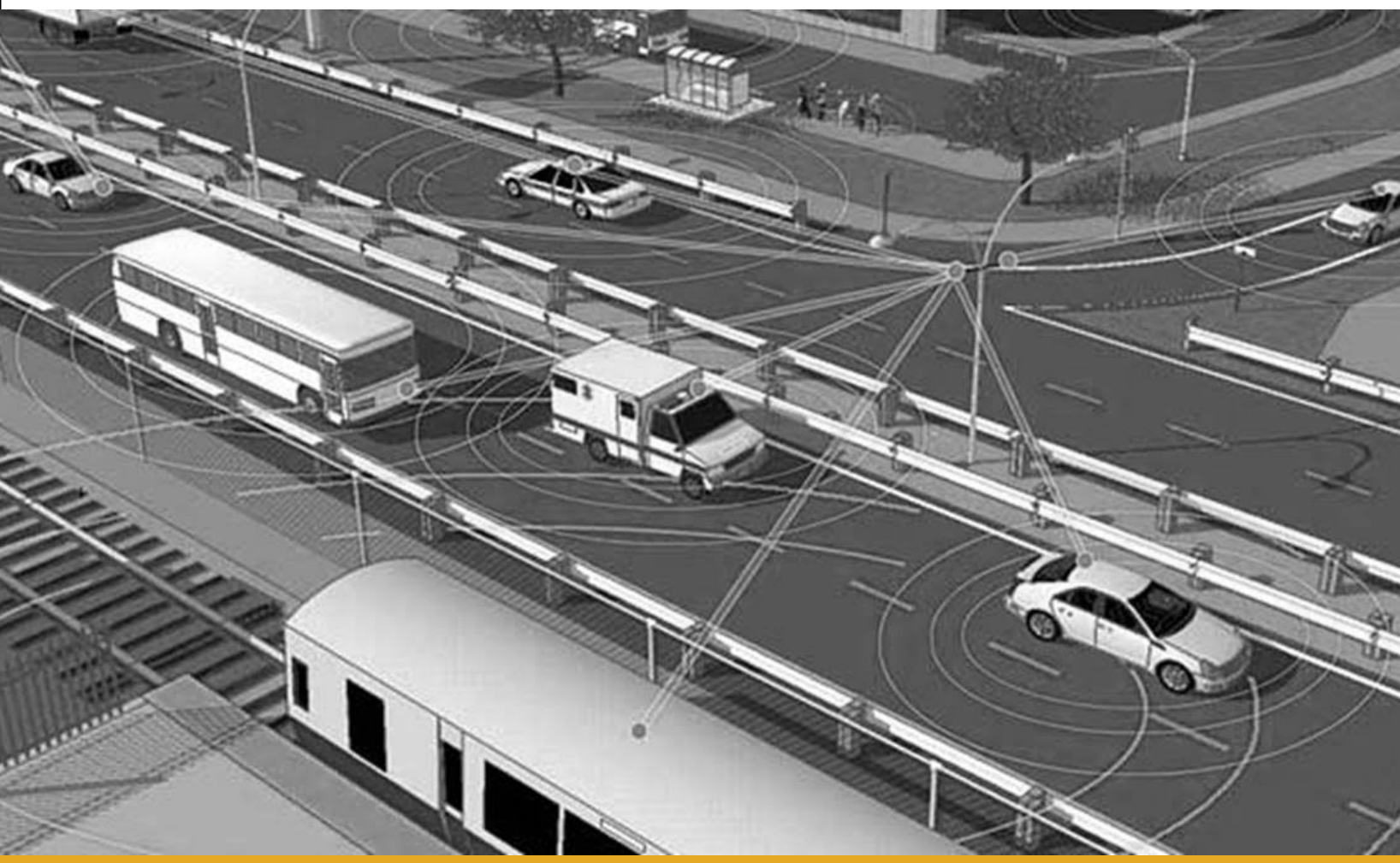
Jacques R. Francoeur
National Transportation Security Center, Mineta Transportation Institute

SJSU SAN JOSÉ STATE UNIVERSITY

MTI MINETA TRANSPORTATION INSTITUTE

Managing Cyber Risks & Business Exposure in the Surface Transportation Ecosystem

Jacques R. Francoeur



MINETA TRANSPORTATION INSTITUTE

LEAD UNIVERSITY OF

Mineta Consortium for Transportation Mobility

Founded in 1991, the Mineta Transportation Institute (MTI), an organized research and training unit in partnership with the Lucas College and Graduate School of Business at San José State University (SJSU), increases mobility for all by improving the safety, efficiency, accessibility, and convenience of our nation's transportation system. Through research, education, workforce development, and technology transfer, we help create a connected world. MTI leads the four-university Mineta Consortium for Transportation Mobility, a Tier 1 University Transportation Center funded by the U.S. Department of Transportation's Office of the Assistant Secretary for Research and Technology (OST-R), the California Department of Transportation (Caltrans), and by private grants and donations.

MTI's transportation policy work is centered on three primary responsibilities:

Research

MTI works to provide policy-oriented research for all levels of government and the private sector to foster the development of optimum surface transportation systems. Research areas include: bicycle and pedestrian issues; financing public and private sector transportation improvements; intermodal connectivity and integration; safety and security of transportation systems; sustainability of transportation systems; transportation / land use / environment; and transportation planning and policy development. Certified Research Associates conduct the research. Certification requires an advanced degree, generally a Ph.D., a record of academic publications, and professional references. Research projects culminate in a peer-reviewed publication, available on TransWeb, the MTI website (http://transweb.sjsu.edu).

Education

The Institute supports education programs for students seeking a career in the development and operation of surface transportation systems. MTI, through San José State University, offers an AACSB-accredited Master of Science in Transportation Management and graduate certificates in Transportation Management, Transportation Security, and High-Speed Rail Management that serve to prepare the nation's transportation managers for the 21st century. With the active assistance of the California Department of Transportation (Caltrans), MTI delivers its classes over a state-of-the-art videoconference network throughout the state of California and via webcasting beyond, allowing working transportation professionals to pursue an advanced degree regardless of their location. To meet the needs of employers seeking a diverse workforce, MTI's education program promotes enrollment to under-represented groups.

Information and Technology Transfer

MTI utilizes a diverse array of dissemination methods and media to ensure research results reach those responsible for managing change. These methods include publication, seminars, workshops, websites, social media, webinars, and other technology transfer mechanisms. Additionally, MTI promotes the availability of completed research to professional organizations and journals and works to integrate the research findings into the graduate education program. MTI's extensive collection of transportation- related publications is integrated into San José State University's world-class Martin Luther King, Jr. Library.

REPORT WP 18-12

MANAGING CYBER RISKS & BUSINESS EXPOSURE IN THE SURFACE TRANSPORTATION ECOSYSTEM

Jacques R. Francoeur

January 2019

A publication of
Mineta Transportation Institute
Created by Congress in 1991

College of Business
San José State University
San José, CA 95192-0219

TECHNICAL REPORT DOCUMENTATION PAGE

1. Report No. WP 18-12	**2. Government Accession No.**	**3. Recipient's Catalog No.**
4. Title and Subtitle Managing Cyber Risks & Business Exposure in the Surface Transportation Ecosystem		**5. Report Date** January 2019 **6. Performing Organization Code**
7. Authors Jacques R. Francoeur		**8. Performing Organization Report** MTI Report WP 18-12
9. Performing Organization Name and Address Mineta Transportation Institute College of Business San José State University San José, CA 95192-0219		**10. Work Unit No.** **11. Contract or Grant No.** 69A3551747127
12. Sponsoring Agency Name and Address U.S. Department of Transportation Office of the Assistant Secretary for Research and Technology University Transportation Centers Program 1200 New Jersey Avenue, SE Washington, DC 20590		**13. Type of Report and Period Covered** Final Report **14. Sponsoring Agency Code**
15. Supplemental Notes		

16. Abstract

This report focuses on Surface Transportation (ST), both fixed and route-based, and the growing threats to their information technology (IT) infrastructures. As an industry, ST seeks to optimize the movement of people and goods, while ensuring safety and resiliency and minimizing environmental impact. Cyber threats are a powerful medium for those with the political, social, and economic motivations and wherewithal to disrupt and destroy existing ST systems. The ultimate objective is to develop a new paradigm to define, describe, design, and deploy the most effective protection, at the lowest cost, in the shortest time within the limits of available resources. This paper seeks to initiate a critical peer discussion to explore innovation in the cyber protection of ST systems.

17. Key Words Safety and security; security; computer security; information technology	**18. Distribution Statement** No restrictions. This document is available to the public through The National Technical Information Service, Springfield, VA 22161		
19. Security Classif. (of this report) Unclassified	**20. Security Classif. (of this page)** Unclassified	**21. No. of Pages** 29	**22. Price**

Form DOT F 1700.7 (8-72)

Library of Congress Catalog Card Number:
2019930394

Mineta Transportation Institute
College of Business
San José State University
San José, CA 95192-0219

Tel: (408) 924-7560
Fax: (408) 924-7565
Email: mineta-institute@sjsu.edu

transweb.sjsu.edu

011019

ACKNOWLEDGMENTS

The authors thank MTI staff, including Executive Director Karen Philbrick, Ph.D.; Deputy Executive Director Hilary Nixon, Ph.D.; Research Support Assistant Joseph Mercado; Executive Administrative Assistant Jill Carter; and Editing Press for editorial services.

Cover Image Source: US Department of Transportation.

TABLE OF CONTENTS

LIST OF FIGURES

EXECUTIVE SUMMARY

This report focuses on Surface Transportation (ST), both fixed and route-based, and the growing threats to their information technology (IT) infrastructures. As an industry, ST seeks to optimize the movement of people and goods, while ensuring safety and resiliency and minimizing environmental impact. Cyber threats are a powerful medium for those with the political, social, and economic motivations and wherewithal to disrupt and destroy existing ST systems. Yet with current funding levels, often determined as about 4% of the IT budget, the cybersecurity industry struggles to protect organizations in fields ranging from federal and state governments to private industry.

The ST industry's current drive to improve services and reduce costs through automation is rapidly leading to advances that will be even more difficult to protect if security measures are not built-in from the start. It is a truism that soon every physical system will be remotely controllable over the Internet. Yet all systems that are theoretically controllable for legitimate purposes can also be accessed for malicious purposes. The access given to the trusted insider may also provide access to the attacker.

What are the odds of an attack, and how much must be spent in order to prevent one? Attackers need only be successful once; defenders need to be successful every time. The acceptance of this reality results in different security strategies and resiliency response plans.

In order to address the above, this paper follows the structure detailed below:

- **Cyber State of Affairs** provides an overview on the current level of cybersecurity in the ST industry in three sections. The first underlines that a successful cybersecurity initiative is predicated on understanding and modeling the problem completely. It also provides an industry overview of current cybersecurity practices. The second underlines just how inadequate current protection from cyberattacks is. The third proposes a better way of understanding and modeling cyber threats.

- **Managing Cyber Risks and Business Exposure**, also divided in three sections, provides a more detailed approach to understanding various cybersecurity issues and management strategies to abate them. The first section aims to illustrate attackers' motives. The second section identifies typical cybersecurity vulnerabilities and risks faced by organizations. The somewhat larger third section proposes improved management structures and underlines the roles of different departments within a typical organization in helping address cybersecurity issues.

- **Conclusion: Eleven Lessons Learned** summarizes the above two sections into eleven key 'lessons' regarding the current state of cybersecurity in ST organizations and introduces the proposed Surface Transportation Cyber-Protection Model and Reference Architecture detailed in Part B of this paper.

The ultimate objective is to develop a new paradigm to define, describe, design, and deploy the most effective protection, at the lowest cost, in the shortest time within the limits of available resources. This paper seeks to initiate a critical peer discussion to explore innovation in the cyber protection of ST systems.

I. CYBER STATE-OF-AFFAIRS

Cyber systems are virtual and, therefore, difficult to manage. The ephemeral nature of network connections, computers, and digital data makes defining and understanding their inherent risks very challenging. As a result, it is also difficult to justify and quantify the degree of protection and associated level of investment that are needed when the threats are not well-understood.

Understanding the physical world, as opposed to the virtual, is relatively straightforward, since it is tangible and measurable. To affect the real world, it is necessary to get into contact with it. The virtual world removes this constraint, enabling remote access to devices that control physical systems.

Using the cyber world as a means to disrupt real world events has proven to be very effective. For example, the Stuxnet computer worm, considered the world's first digital weapon, is credited with successfully disrupting Iranian efforts to develop a nuclear weapon.[1] Appendix C provides examples of threats or events that demonstrate the implications of poor cybersecurity on the physical operation of railway systems. If cyber security measures are insufficient, disruptive malware can unwittingly be distributed to vast numbers of endpoints overnight.

This chapter is divided into three sections. The first, entitled The Truth of the Matter Matters, describes the two major software engineering approaches to cybersecurity and illustrates how more and more physical and logical systems are remotely controllable via an Internet connection. The second, The New Normal is Inadequate, illustrates the large degree to which current cybersecurity practices, especially in the Surface Transportation (ST) industry, are lacking. The third, There Must Be a Better Way, provides a high-level overview of the potential solutions that are explained in greater depth later in the paper.

THE TRUTH OF THE MATTER MATTERS

For most ST organizations today, an imminent cyberattack would result in nothing short of a disaster. Although some comfort can be gained in the knowledge that peers within the ST industry are not alone in this issue, the reality is that most companies most likely underinvest in cybersecurity and hence are dangerously exposed.

> The question is not: Have we done enough? The answer is clear**—no one has done enough.**
>
> The question is: **What do we do about it now?**

In software engineering, there are two schools of thought on designing cybersecurity: secure-by-design and secure-by-default. Secure-by-design systems are designed from the "ground up" to be secure from threats, while secure-by-default systems are designed to have the default configuration settings be the most secure settings possible, sometimes at the expense of user-friendliness.[2] Yet both design patterns are rarely found in current ST systems, requiring security to function as a Band-Aid, which increases the complexity of the necessary security measures, downgrading performance and user experience.

Increasingly, physical systems are being virtually controlled by applications accessed over the Internet. A common example of this phenomenon in surface transportation systems is the use of industrial control systems, which are commonly used to control subways and other rail infrastructure. If these applications are accessible over the Internet for legitimate purposes, then they can be compromised and accessed for malicious purposes as well. The only thing that separates the two is intent.

The attempt to provide security does not always entail adequate protection. There are many reasons why protection is especially difficult to achieve, even when security has been provided. Ineffective security often results from basic factors such as improper configuration of security measures and poor basic information technology (IT) hygiene. Inadequate funding is also responsible for ineffective security, as it naturally degrades over time. Security management often suffers from inadequate communication and measurement, which is then exacerbated by the difficulty of tracking threats.

Protecting a complex organization with bad IT is impossible. Humans are often the weak link for specialized social engineering attacks. An example of this is ransomware attacks, where IT or other employees are baited into clicking on a link which subsequently installs malware on their system, potentially allowing an infection of other systems within the organization. The malware then allows the attacker to steal data and hold it at a ransom. Cybersecurity is now far too complex to be managed by humans, yet the main tool used in security today by practitioners is Microsoft Excel.

THE NEW NORMAL IS INADEQUATE

Fortunately, through breach notification laws, we are learning of breaches almost daily. Unfortunately, the high exposure to these breaches has numbed our senses. The recent breach of a credit score company, releasing the detailed financial data of 143 million Americans, reflected a new low in standard of care.[3] In the ST domain, a 2016 breach exposing 57 million accounts of a global taxi technology company remained undisclosed for more than a year.[4] The company later paid a $100,000 ransom to the hackers to delete their copy of the stolen data.

The question after a cybersecurity breach asked by those who are harmed is always: Did they do enough? In most cases, more should have been done, and lawsuits claiming inadequate care are routine. Historically, most breaches have been traced back to the exploitation of IT vulnerabilities that were well known and for which patches were available for over a year (see Appendix B).

The IT vulnerabilities in the transportation domain are no different. Transportation providers (both public and private) are dependent on IT systems similar to those employed by other industries, and thus are just as likely to under-invest in cybersecurity measures. Even when the proper investments are made, there is no reason why a malicious Organized Attacker Group, given sufficient time and resources, cannot take control of a critical surface transportation system that is legitimately accessed and controlled over the Internet.

THERE MUST BE A BETTER WAY

There are many reasons why security has failed to provide adequate protection. Security cannot provide protection at all costs, because such a goal is financially unfeasible. There must be a reasonable level of investment to provide adequate protection, meeting the security expectations of customers at a price they are willing to pay.

Security after design—namely, where security is introduced as an after-thought—is less effective and costlier to maintain than security-by-design—namely, where security is integrated into the architecture of the IT system from the ground-up. Unfortunately, when it comes down to a choice between more features in a system and more cybersecurity, security is often the loser. In these all-too-common cases, security must be applied after design, making the asset more difficult to protect.

Additionally, the importance of maintaining good system hygiene and a minimal, well-hardened attack surface has also been ignored. With most of today's compromises resulting from the exploitation of known vulnerabilities in IT assets, keeping them securely configured and patched is a critical first step towards better hygiene. Once done, it is advisable to understand the points of vulnerability—or the "attack surface"—in an IT system. The attack surface relates to the IT devices whose IP addresses are exposed to the Internet. The number of these public IP addresses should be minimized and highly controlled. Such public facing devices should be securely configured and any modification detected.

Today, given the early stages of security automation, processes are manual and humans are "in-the-loop" in most aspects of security. Given the severe shortage of experienced security professionals and the number of open positions, a large number of inadequately trained practitioners have and will continue to enter the space. At the same time, the complexity, interconnectedness, and sheer size of existing systems has outpaced most humans' ability to effectively secure them.

To address these problems, the first step is for humans to identify the complexity and size of the systems and the degree to which they are automated. Additionally, measures to closely track the size, interconnectedness, and weak points of existing systems must be put in place. The next step is then to visualize and analyze such information, which will allow for better understanding of security weaknesses across all strata of ST organizations. Additionally, this level of understanding will allow security systems to be automated, allowing for more efficient counter-hacking measures.

Unfortunately, current cybersecurity best practice standards and regulations and the ability of most organizations to implement them fall short.[5] In response, this paper proposes the basis for an enhancement of how security controls are defined, interpreted, measured, visualized, and communicated. The proposed enhancement will greatly improve existing methods to define, measure, and represent an organization's state-of-security, state-of-protection, and state-of-compliance, hence allowing for the ability to develop and deploy more effective countermeasures to security threats.

The proposed enhancement is a taxonomy advancement called the Security Control Expressions (SCE). A SCE explicitly describes the relationship between security delivered by security assets and the protection received by business assets. Cyber threats and countermeasures can be expressed, associated, measured, visualized, and analyzed in powerful new ways. The impact can be transformational for the security industry, resulting in the ability to protect surface transportation systems at adequate levels as soon as reasonably possible.

II. MANAGING CYBER RISKS AND BUSINESS EXPOSURE

The preceding sections sought to establish awareness of the many facets of the ST industry's cybersecurity issue, an idea of where organizations currently are, and what they are facing. Yet establishing and defining the current issues in the field is not enough.

If cyber risks are not on the minds of business leaders and ST organizations, then new approaches to describing the threats and potential damages must be devised. The best way to do so is to express the potential impact in financial terms, such as net income exposure and current and future revenue growth exposure. When viewed through the lens of the bottom line, executive leaders at ST organizations, both public and private, can compare the costs and benefits of cybersecurity with other business initiatives. By changing the way in which the need for cybersecurity is presented, the urgency of the issue can be stated much more clearly.

Unfortunately, it is challenging to express cyber risks in financial terms. This communication barrier is responsible for the chasm that exists today between those who work on technical issues and those who work in the business realm. This divide between the fiduciary business layers and IT security is largely responsible for the universal underinvestment in security. Addressing the current issues in cybersecurity management, especially in the ST industry, requires addressing many common misconceptions. Key misconceptions that routinely endanger cybersecurity are addressed below.

The first common misconception is that security is the sole responsibility of the Chief Information Security Officer (CISO). This formal position is where all matters cyber are centrally managed and reported. However, it is more productive to have a business and risk-focused person who can synthesize and communicate to senior executives in language aligned to their concerns. An organization without such a position does not have the necessary resources to improve their standard-of-care. Cybersecurity is a complex field and requires good management practices to avoid the typical waste cycle of security investments.

While CISOs certainly serve a critical role in cybersecurity, there are many other important responsibilities that are typically the responsibility of other executives. The objective is to manage cyber risk, and there are several risk treatment methods. For example, setting and establishing reasonable risk acceptance levels is a fiduciary responsibility that guides businesses on the question of the limits of the risk they should accept. Risk indemnification, transfer, and avoidance risk treatment measures are the purview of the legal team and the General Council. A common error is that CISOs commonly report to the Chief Information Officer (CIO). Because the CIO is concerned with rapid advancement and cost reductions rather than cautiousness and the inherently costly nature of cybersecurity, it is a conflict of interest for the CISO to report to the CIO. For this reason, the CISO should instead report to the General Council or the Chief Risk Officer, which will be able to better handle the difficult and costly tradeoffs regarding cybersecurity.

Stop the intent of the attack.

Stop them from getting out, not from getting in.

A second reality that must be accepted is the recognition that it is virtually impossible to stop a persistent, well-resourced, and sophisticated attacker. It is therefore important to focus beyond denial-of-access measures (also known as “fence building”) to hackers and other security threats, but to also develop the capabilities to constrain movement, detect anomalous behavior, and ensure that attackers cannot exit systems with important information. These counter-measures require a different set of security skills and technologies compared to simply denying access. compared to simply denying access. These skills are centered around data analysis, anomalous behavior detection, and fraud prevention.

It is important to think strategically and plan tactically about how to stop the intent of the attack, as opposed to only the attack itself. The attack has a motive, and it is not limited to just getting in. One way to understand the motive of the attacker is by tracking their movements once they have gained access to your system. However, it takes a mature organization to track an attacker without the attacker’s awareness, since security response actions provide indicators to the attacker that they have been detected. Once an attacker is aware that they are being tracked, they become much more difficult to find as they often go into “sleep” mode, yielding little information to the trackers watching them.

The following sections provide a detailed outline of the problem and the approaches to solving it. First, the different motives of potential attackers are discussed in the following subsection, entitled “Why Would They Attack Me?”. Next, “Cyber Risks Created by Cyber Threats” details specific cybersecurity risks to organizations. Lastly, “Cyber Risk Management and Achieving a Reasonable Standard-of-Care” outlines a management structure to effectively handle cybersecurity at all stages of a potential attack, assigning roles to each department within a typical ST organization.

WHY WOULD THEY ATTACK ME?

The following section describes distinct types of cybersecurity threats faced by the ST industry. Each type of threat includes either possible targets within ST systems or successful attacks targeting the particular vulnerability. These threats are summarized below in Figure 1.

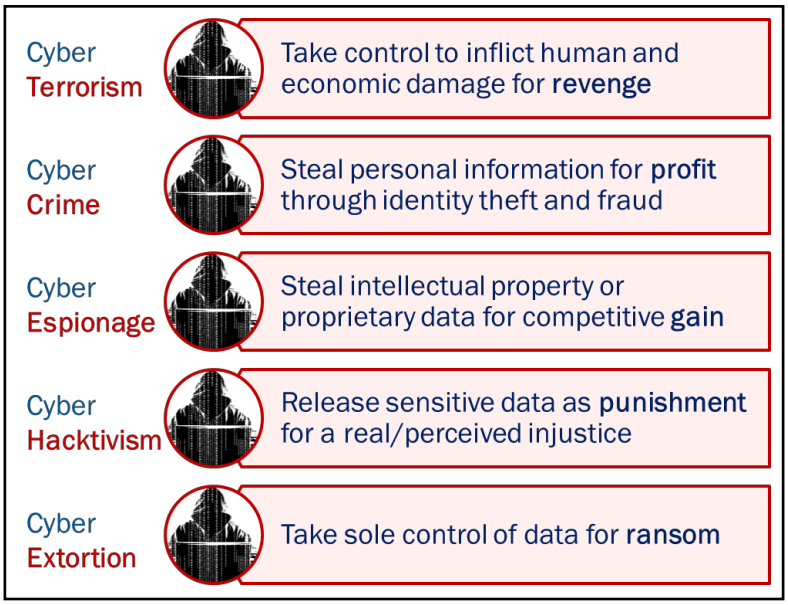


Figure 1. Cyber Threats by Motive & Intent

- **Cyber Terrorism**: The intent is to disrupt the target's physical systems by remotely taking over control systems and either shutting them down, opening them up, destabilizing them, or otherwise operating them beyond design limits. The impact of a cyber-terrorist taking control of a target's IT system is dependent on the design and operational characteristics of that system, but it has been shown that logical (virtual) actions can lead to real world, kinetic events. An example of a specific threat of this type in the ST industry is attacks on rail balise systems, which convey real-time information about train and track positions. These systems have been found to have significant security vulnerabilities in existing literature.[6]

- **Cyber Crime**: The intent is to steal health, financial, and personal information of employees and customers for money through identity theft and financial fraud.

- **Cyber Espionage**: The intent is to steal transportation technology secrets, intellectual property and proprietary information, such as pricing, for competitive gain, lowering their own costs of development and shortening the time it takes to enter the market with these new technologies.

- **Cyber Hacktivism**: The intent is to dispense punishment for a real or perceived injustice. This can include disclosing confidential data or interrupting the normal operation of a ST system. An example of this came in 2011, when hackers infected a website for the Bay Area Rapid Transit police union, and released the personal information of over 100 officers to protest the agency's shutting down of Wi-Fi in underground tunnels.[7]

- **Cyber Extortion**: The intent is to take sole control of data for profit, make it unintelligible by malicious encryption, and demand compensation for its reliable recovery. One example of such an attack in the ST industry is the 2016 San Francisco

Municipal Transportation Agency ransomware hack, where hackers compromised more than 2,000 servers at the agency, holding confidential information at a ransom of 100 bitcoin.[8]

It is essential that we have an unbiased, scientific view of the cyber threat landscape. Appendix B references the U.S. Secret Service and Verizon data breach investigations, now in their tenth year. These documents exemplify state-of-the art thinking and an unbiased analysis of the current cyber threat landscape.

CYBER RISKS CREATED BY CYBER THREATS

What damages can result from the above threats, if realized? The following are ST-specific risks that can be realized from cyber threats. The nature of the damages varies by the impacted asset. Risk is proportional to the likelihood of the compromise being realized multiplied by its impact. Each risk detailed below is associated with a potential outcome or concrete consequence of an attack that has been carried out on a ST system in the past. These risks are displayed in Figure 2.

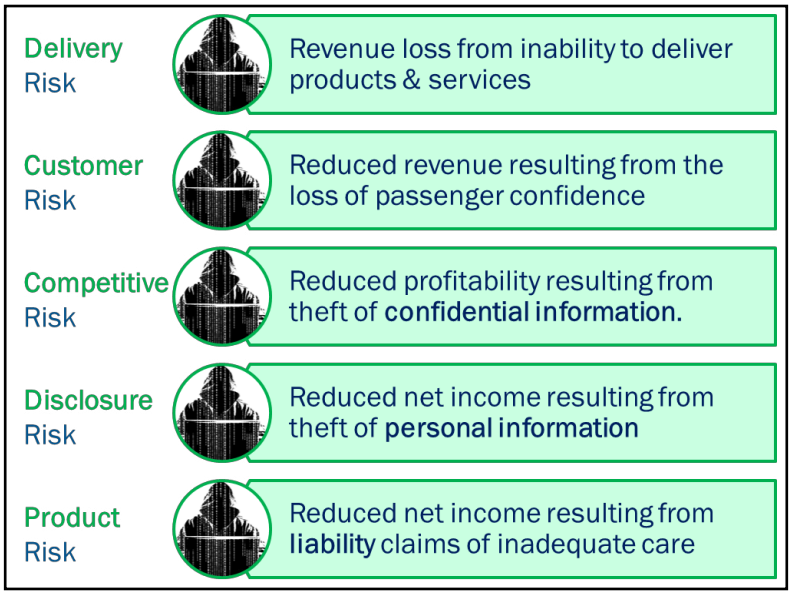


Figure 2. Cyber Threats Creating Business Risks

- **Delivery Risk**: The inability to deliver and operate products and services; this is largely a risk incurred by cyber terrorism. An example of this risk being realized occurred in a 2014 Michigan experiment, where researchers were able to break into a local network of traffic lights, gaining control of almost 100 intersections.[9]

- **Customer Risk**: The loss of passenger confidence in the safety and reliability of system after a cybersecurity breach. For many transportation agencies, however, the lack of competition means this risk is less significant compared to others. Those relying on public transportation as a primary mode of transportation rarely have alternative options.

- **Competitive Risk**: Financial loss resulting from theft of trade secrets, proprietary information, and intellectual property.

- **Disclosure Risk**: The theft and unauthorized release of personal customer and employee data. Although this normally regards customer data, as in the aforementioned taxi company breach, employee data is a target as well; in 2016, ISIS-affiliated hackers broke into a New Jersey Transit police website and published officers' personal information and names on Twitter.[10]

- **Product Risk**: Financial loss resulting from liability claims of inadequate care in preventing system compromises.

The risks defined above can be separated into two categories. Delivery and product risks largely pertain to the physical components of a surface transportation system, exemplified in the examples provided of such risks being realized. Delivery risk can be thought of as impacting the operation of existing components, while product risk can be thought of as impacting the design and integrity of the components themselves. The other risk categories pertain to breaches and leaks of sensitive data, be it the personal data of employees or customers, or trade secrets—for example, in the autonomous vehicle industry. Appendix A contains further information on risks and risk management strategies specific to rail infrastructure.

CYBER RISK MANAGEMENT AND ACHIEVING A REASONABLE STANDARD-OF-CARE

When realized, the above risks create financial exposure. Financial exposure is the cost of liabilities related to claims of inadequate care, breach-related costs where customers must be notified and protected, and fines from regulators, which vary depending on the findings of the incident. Financial exposure does not include the costs of conducting day-to-day security.

Addressing and managing this financial exposure is one of the key foci of the following two subsections. Additionally discussed are concrete management structures and processes that are necessary to achieve an appropriate standard-of-care—the level of due care exercised by agencies, operators, and companies—in ST organizations.

Stakeholder Journey to Reasonable Standard-of-Care

Figure 3 illustrates the management cycle of assessing and improving the cybersecurity standard-of-care, and consequently reducing residual exposure. Each step in the process is associated with the specific department within an organization that is responsible for it (left of the figure).

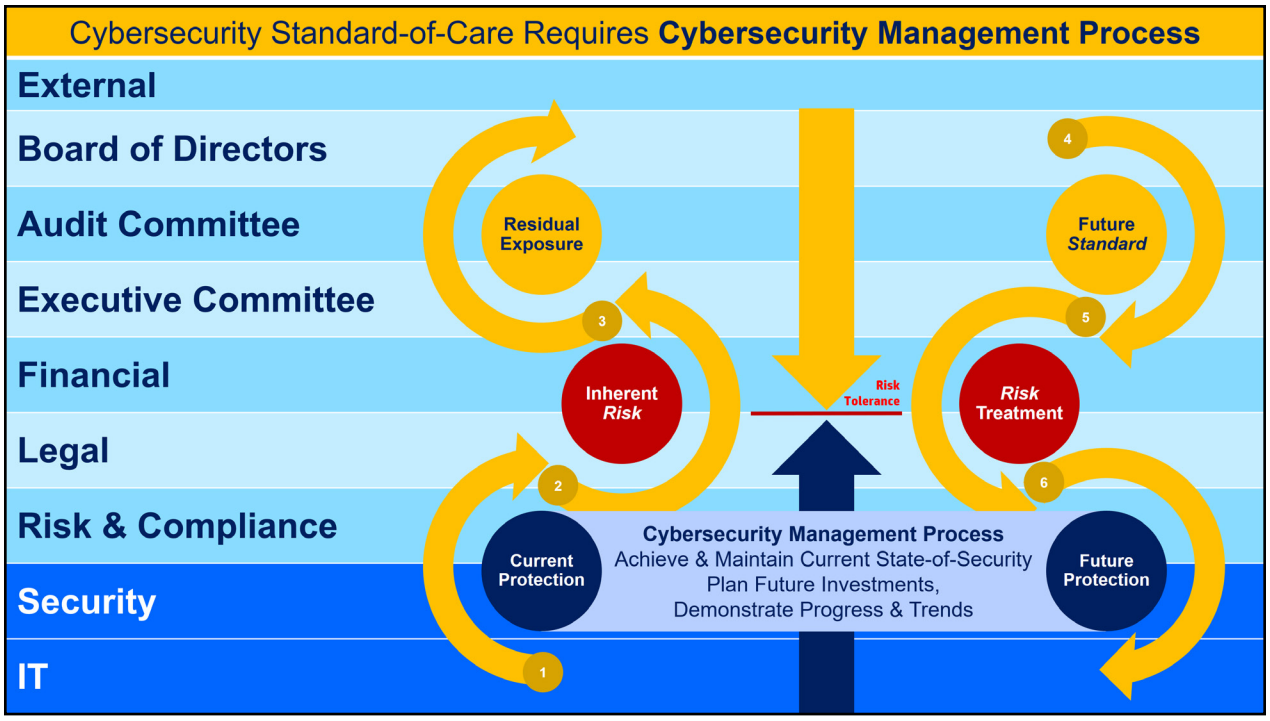


Figure 3. Standard-of-Care Evaluation Cycle

Key to Figure 3 are the two distinct sides. The left side illustrates the current level of protection, its associated risk, and the residual exposure. The right side illustrates the desired future standard-of-care, the risk treatment, and methods for future protection against that risk. Assessing levels of protection, both current and future, is the role of the Security, Risk & Compliance, and IT departments. Transferring this information to tangible financial and legal ramifications is the role of the Financial and Legal departments. Interpreting this data and deciding on the acceptable exposure and standard-of-care is the role of the Board of Directors, Audit Committee and the Executive Committee.

The first step in the journey to an acceptable standard-of-care is assessing the residual exposure, defined as the potential financial loss incurred if the accepted risk is realized. This exposure level should reasonably allow an organization to recover after a successful attack. To assess whether the level of residual exposure is appropriate, a quarterly review and decision cycle must be put in place in order to keep the standard-of-care up-to-date with the organization's infrastructure. If an organization has excessive residual exposure, and potential financial loss from an attack is not financially recoverable, then the organization must improve the standard-of-care.

Key to the concept of residual exposure is understanding the role and size of the ST organization within a broader ecosystem of services and other organizations, knowing the potentially valuable assets of one's organization, and the motives of a potential attack. By knowing one's state of security and therefore how protected business assets are, one can estimate the residual exposure.

Based on the result of the assessment, fiduciary management determines whether the nature and level of risk and exposure is reasonable or excessive. If deemed excessive, investments are made to improve the standard-of-care. This process includes addressing the sources of potential risks with different treatment options and investing in in risk mitigation. It also includes selecting and deploying additional protection measures designed to protect against specific threats.

The overall objective of this cycle is to ensure the adequate protection of the most critical dependencies of the most valuable processes with the highest exposure. This strategy ensures that with limited time and resources, the most important risks are taken care of first. The process starts with understanding which assets underpin which type of risk, level of severity, and likelihood. Once this is understood, measures can be taken to reduce both the likelihood and impact.

Cyber Response by Stakeholder and Attack Stage

An accurate, clear, and concise set of terms describing the processes of cyberattacks and their induced responses is key to improving responses to and reducing the costs of addressing cyber threats. This section outlines a set of terms defining the progressive stages of a successful attack, the responses incurred at each stage of an attack, and the roles of each stratus of an organization during a stage of attack.

Before identifying responses to an attack, it is important to understand how a cyberattack occurs. Defined below are the progressive stages of a successful attack.

- **Attack**: Organizations are attacked thousands of times a day, even tens of thousands of times if they are high-value targets. For example, financial, health, or technology companies typically house valuable personal information and intellectual property, making them frequent targets of cyberattacks.

- **Compromise**: An attack has been successful and the attacker is “inside the network” performing unauthorized activities with malicious intent. Some organizations have no idea if they are compromised or not.

- **Incident**: Once detected, the compromise becomes an incident and incident response is initiated. Less mature organizations often attempt to shut down impacted systems and remediate immediately, telling the attackers that they have been found. More mature security organizations start a cat-and-mouse game to contain the attacker without the attacker knowing, with the objective to learn their intent and discover the full implication of the compromise.

- **Breach**: The objective of responding to an incident is to prevent it from becoming a breach. A breach should not be confused with being compromised. Rather, breach is strictly reserved as a term that implies a strong legal response must be triggered. If an incident was successfully contained, it does not constitute a breach.

The only opportunities for an organization to respond to an attack are during the compromise and incident stages. Any attempt to engage with attackers after an attack is successful is risky and potentially illegal, as indicated in an example cited earlier in this paper, where a global taxi technology company ended up complying with a $100,000 ransom payout to hackers.

Since the form of the risk and corresponding countermeasures vary by attack stage, it is best to look at cyber risks as the attack materializes, progresses, and changes. Based on this approach, appropriate responses by different stages are illustrated in Figure 4, and are as follows:

Figure 4. Cyber Response by Attack Stage

- **Before Stage**: The objective is to prevent an attack from becoming a compromise. This first response stage focuses on governance and building a corresponding security program (i.e., an ability to protect) that is deemed reasonable by key external stakeholders. Therefore, responses in this stage are focused on 'fence building,' with the objective of keeping the attackers out. However, at a certain point, additional investments in such security measures will have diminishing protection returns. At that point, a shift in strategy to the next stage of responses is recommended.

- **During Incident Stage**: The focus of this stage is to contain the incident and prevent it from escalating into a breach, the successful intent of the attack. If the intent of the attack also triggers a public event, such as Breach Notification Laws, it is a breach that also causes reputational damages. This moves the response to the next stage.

- **During Breach Stage**: The focus of this stage is to accomplish everything in the previous stage while dealing with authorities, regulators, investors, and customers without causing additional damages. As a result, we often see a significant shift in resources from technical to legal and communication at this stage.

- **After Stage**: The objective of this stage is to contain breach damages and rebuild. The effects of the breach stage often linger beyond the days in which the attack is "in the news," often years. Less tangible values such as trust and reputation lost can take a very long time to rebuild. This stage also involves legal liability claims, on-site auditor presence, and annual audits for several years.

Based on the cyber risk management decision cycle, attack stages, and response stages as discussed previously, Figure 5 illustrates a corresponding response matrix, broken down by stakeholders, underlining the role of each department at an organization in cyber risk management.

Cyber Risk Management Response by Stakeholder & Stage				
Stakeholder	Before	During		After
	Before Compromise (Govern, Budget, Build)	During **Incident** (Respond & Remediate)	During **Breach** (Contain & Rebuild)	**After Breach** (Contain, Standard-of-Care)
Directors	Cyber **Fiduciary** Standard-of-Care Governance	Cyber **Material** Incident Oversight	Cyber **Breach** Oversight	Cyber **Standard-of-Care** Planning
Audit	Cyber **Audit** Compliance Governance	Audit **Incident** Investigation	Audit Breach **Investigation**	Cyber **Care** Oversight
Business	Cyber **Business** Governance	Business **Breach** Preparedness	Business **Preservation**	Cyber **Business** Planning
Financial	Cyber **Financial** Governance	Incident **Financial** Tracking	Breach Financial **Payout**	Cyber **Financial** Planning
Risk	Cyber **Risk** Management	Cyber **Incident** Response Evaluation	Cyber **Breach** Response Evaluation	Cyber **Risk** Planning
Legal	Cyber **Liability** Management	Legal **Breach** Preparedness	Breach **Damage** Containment	Cyber **Liability** Planning
IT	IT **Security** Operations Program Management	**IT** Incident Response	IT Breach Response **Evaluation**	IT **Security** Program Planning
Security	Cyber **Security** Program Management	Incident Security Response	Security Breach Response **Evaluation**	Security **Program** Planning

Figure 5. Response by Stakeholder and Response Stage

III. CONCLUSION: ELEVEN LESSONS LEARNED, AND A CYBERSECURITY MODEL FOR SURFACE TRANSPORTATION

Society's commercial track record for security-by-design and security-by-default in logical systems security is, unfortunately, not very strong in most cases. This is due in part to the perceived unwillingness of the end customers to pay for the higher cost of security-by-design. This trend is changing as the pain and damages from cyber threats get closer to the consumer.

If the past is any indication, surface transportation systems will rush to innovate without fully understanding the cybersecurity implications, let alone designing and implementing secure-by-design or secure-by-default systems. The further security measures are from the built-in design of a system, the more complex and difficult such a system is to protect.

Product liability and the standard of due care is interpreted differently in the physical and digital worlds. Harm in the physical world is clearer than "digital" harm. Providers of surface transportation systems are more likely to be liable for product safety failings than a software platform provider would be for insecure third-party applications.

Relying on old paradigms and refusing to accept new truths make the job more difficult and are a sure way to destroy value quickly. Defining key assumptions and presumptions accurately will greatly improve the effectiveness of the strategy and resulting security posture. Below are eleven key lessons learned from previous sections of the paper and important truisms of the cybersecurity industry.

1. **Prime Directive:** Not all assets are of equal sensitivity, criticality, or business value. Given scarce cybersecurity resources, the most valuable assets should be protected first, the second-most valuable second, and so on. The idea is that, by the time resources have been exhausted, the most important system elements have been adequately addressed. The Security Scarce Resource Prime Directive, in the text box above, should guide where to invest in cybersecurity. This assumes a knowledge of assets, where they are, and what they are doing.

Security Scarce Resource Prime Directive

"Ensure the adequate protection of the most critical dependencies, of the most valuable processes, with the highest exposure."

2. **Presumption:** Today, security strategy must build sufficient resiliency to continue to deliver the product and services securely to customers while being compromised. This is the reality, and no security officer can be held to the standard to prevent any and all possible attacks. Most organizations contain many assets of value to attackers. Organizations of value are under constant attack and therefore in a constant state of response to multiple incidents, fraud attempts, and investigations. This is simply the reality. This presumption shifts security investments towards monitoring internal activity, detecting unauthorized behavior, and responding with preventative controls to stop the activity.

3. **Security is a Degree-of-Difficulty:** Any target can be compromised given enough time and resources. The easier it is to compromise a target, the more likely less sophisticated and resourced attackers will do so. How difficult should it be? There is no device on an organization's network that cannot be compromised if it is accessible and controllable via that network. If it can be accessed for legitimate reasons, it can be accessed for malicious reasons. The more difficult it is to accomplish each stage of the attack, the less likely it is to be successful. As the difficulty level increases, the number of attackers with the skills, resources, and persistence to accomplish the compromise decreases.

4. **Stop Them from Getting Out:** It is more critical for a business to stop the intent of the attack, rather than the attack itself. Stopping hackers from getting out of the system with critical data is more important than trying to keep them from getting in. This is key to preventing an incident from escalating to a breach.

5. **Why Would I Be Attacked:** As discussed in Section 3, understanding the vulnerability of one's organization is largely a matter of understanding one's role in the larger ST ecosystem and the assets that are of value to potential hackers.

6. **Fix IT First:** Companies rarely maintain core IT best practices. Maintaining good software and hardware hygiene is half the security battle. The risks and need for security originates in large part from the major challenges of protecting bad IT. And bad IT in most cases is a result of underfunding. More sophisticated countermeasures to address more sophisticated and persistent attackers with more sinister intents are not effective if the basics are left wide open and a teenage attacker is able to penetrate an organization.

7. **Minimize and Harden Attack Surface:** An organization's "attack surface" is defined by the number of Internet-facing IP addresses and their connected devices, each of which is a potential point of vulnerability to be exploited by an attacker. The key is to minimize the number of public IP addresses and ensure that connected devices are securely configured, cannot be modified without detection, and all applicable software patches are up to date. The likelihood of an attack is strongly associated with the size and condition of the attack surface.

8. **Protection versus Security:** Businesspeople care about protection; security people care about security. Security delivered does not equal protection received. Business assets are under threat, and whether a security technique to mitigate that threat is effective or not, it must be verified using accepted test procedures, preferably conducted by an independent evaluator. A security technology can be operating "effectively" (as designed), but the efficacy of the technique against the threat may be poor. For example, detection of known malware will be 100% effective in detecting the exact same malware, but will detect almost no new attacks, because the attack signature of almost every new attack is different.

9. **Internal vs External Control Frameworks:** External frameworks are "one size fits all," objective-level security control sets that either organizations should comply

with (according to industry standards) or organizations shall comply with (according to government regulations). There are many external frameworks to choose from, and they evolve on a periodic basis.[11] There is nothing "wrong" with these control frameworks, except that they may not align with the nature of a business and specific risk profile, which, in turn, highly depends on the nature of core assets and activities. An internal framework provides alignment between the security program, the business, and the risk communication.

10. **Compliant vs Secure:** Out of a scarcity of resources and a desire to reduce complexity and duplication, organizations sometimes adopt a well-known and widely accepted external framework as their internal enterprise control framework. In doing so, they avoid the costs and time involved with managing another specialized, internal framework by complying with the standards of an external framework—an approach sometimes called security-by-compliance. However, a compliant environment is not necessarily secure. But it is almost certain that a secure environment is always compliant. Therefore, it is highly advisable that any organization should adopt an internal security control framework optimized to their intrinsic character and aligned to risks to their net worth, current revenue, and revenue growth. These business priorities are translated into Management Business Objectives and managed through to delivery and success. The internal framework should be based on a set of Management Security Objectives tied to each of the business objectives with the goal to protect it.

11. **Approach to Security:** Each leader will have a somewhat different intrinsic approach to cybersecurity determined in part by their personality, education, and past management experience. These differences will, in turn, influence management methods, communication styles, and approaches to building a security program, or lack thereof. Examples of approaches include: a technology and risk mitigation approach, where the focus is on IT measures to reduce the likelihood of a compromise; a legal, risk averse, and indemnification approach, where legal instruments such as contracts to specify onward care obligations are used to assign responsibility outside the organization to limit exposure; a check-list and security-by-compliance approach, where external compliance regulations drives the nature of the security program; and a business and risk acceptance approach, where business tends to take on excessive risks. When only one approach is dominant, other types of risk are inappropriately addressed and under-managed. It is important to seek the right balance of risk treatment measures provided by specialized experts while also ensuring a powerful, accountable and conflict-of-interest-free reporting chain.

To address the current lack of adequate cybersecurity in ST organizations, Part B of this paper proposes a Surface Transportation Cyber-Protection Model and Reference Architecture, which outlines the assets specific to transportation systems that have the potential to be compromised by hackers. This model and reference architecture incorporates the motives and risks discussed above, and integrates the following essential considerations:[12]

- **Hybrid**: Physical and cyber systems, since cyber systems increasingly control physical systems.

- **Multi-disciplinary**: Technical, legal, regulatory, and fiduciary aspects of system design and management.
- **Integrated**: Moving from the strategic to the tactical and moving from objectives to implementation techniques.
- **Community-based**: Participant ecosystem roles and responsibilities.
- **Standardized**: “One Ecosystem Protection” provides security to entire systems.
- **Multi-Regulatory/Standard-Based**: Adequate protection that meets all external security regulatory and standards.
- **Demonstrable**: Measurable across a spectrum of perspectives to increasing degrees-of-precision.

The Model is composed of three key elements. The cyber threat component provides the ability to understand potential threats. The cyber protection component allows organizations to model courses of action and countermeasures to threats. The surface transportation model identifies the common potential layers of attack in surface transportation systems.

Each element of the model has an underlying reference architecture, that is, a framework through which it is modeled and understood. The cyber threat reference architecture illustrates the steps of a successful cyberattack. Its cyber protection counterpart illustrates how to defend against each one of these steps. The surface transportation reference architecture points to specific infrastructural weaknesses within each layer of a surface transportation system.

Through a holistic model such as the above and better understanding of key cybersecurity concepts and attack processes, we hope to foster an interdisciplinary debate on strategies for mitigating and managing cyberattacks on surface transportation topics. We also hope to underline the sheer lack of and need for stronger security for both physical transportation systems and the data associated with them.

APPENDIX A: RAIL SECURITY GUIDANCE

1. US Government: DHS: Office of Cyber and Infrastructure Analysis (OCIA): https://www.dhs.gov/office-cyber-infrastructure-analysis

2. Best Practice Recommendations: https://ics-cert.us-cert.gov/Recommended-Practices

3. The Future of Smart Cities: Cyber-Physical Infrastructure Risk. https://ics-cert.us-cert.gov/sites/default/files/documents/OCIA%20-%20The%20Future%20of%20Smart%20Cities%20-%20Cyber-Physical%20Infrastructure%20Risk.pdf

4. Government of United Kingdom: Rail Cyber Security Guidance to Industry, February 2016: https://www.rssb.co.uk/Library/improving-industry-performance/2016-02-cyber-security-rail-cyber-security-guidance-to-industry.pdf

5. TRB's E-Circular 226: Transportation System Resilience: Preparation, Recovery, and Adaptation. Benefits and Needs for an Integrated Approach to Cyber–Physical Security for Transportation, Rae Zimmerman, New York University Wagner Graduate School of Public Service; Michael G. Dinning, U.S. Department of Transportation Volpe Center: http://onlinepubs.trb.org/onlinepubs/circulars/ec226.pdf

6. Protection of Transportation Infrastructure from Cyber Attacks: A Primer: http://www.trb.org/Main/Blurbs/174382.aspx

7. Security and Privacy Controls for Federal Information Systems and Organizations, Rev 4: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

APPENDIX B: UNDERSTANDING THE THREAT LANDSCAPE

State-of-the-art thinking and unbiased analysis of the threat landscape based on actual breach forensics: US. Secret Service and Verizon data breach investigations report, now in its tenth year: https://www.verizonenterprise.com/verizon-insights-lab/dbir/

APPENDIX C: RAIL-RELATED INCIDENTS

1. City of Lodz, Poland tram system hacked by a 14-year-old schoolboy, causing derailment and injuries, 2008: http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html

2. Train virus disrupts signaling, dispatching result in delays across eastern US, 2003: http://www.cbsnews.com/news/virus-disrupts-train-signals/

3. WannaCryRansomware attack impacts Germany's Deutsche Bahn system, ransomware message appears on station screens, May 2017: https://www.us-cert.gov/ncas/alerts/TA17-132A; http://www.telegraph.co.uk/news/2017/05/13/cyber-attack-hits-german-train-stations-hackerstarget-deutsche/

4. "The Indian Railway Minister, Suresh Prabhu has said that ensuring cyber security of the railway's in the day to day operations is one of the most important priority," July 2017: http://www.ehackingnews.com/2017/07/railways-to-focus-on-cyber-security.html

5. UK Rail Infrastructure under Attack, 2016: https://www.telegraph.co.uk/technology/2016/07/12/uk-rail-network-hit-by-multiple-cyber-attacks-last-year/

ABBREVIATIONS AND ACRONYMS

ST	Surface Transportation
IT	Information Technology
SCE	Security Control Expressions
CISO	Chief Information Security Officer
CIO	Chief Information Officer

ENDNOTES

1. Ralph Langner, “Stuxnet: Dissecting a Cyberwarfare Weapon,” IEEE Security & Privacy 9, no. 3 (May 2011): 49-51.

2. Chad Dougherty, Kirk Sayre, Robert Seacord, David Svoboda, and Kazuya Togashi. *Secure Design Patterns* (CMU/SEI-2009-TR-010), Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2009, http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9115.

3. “The Equifax Data Breach,” Federal Trade Commission, accessed October 19, 2018, https://www.ftc.gov/equifax-data-breach.

4. Mike Isaac, Katie Benner, and Sheera Frenkel, “Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data,” *New York Times*, November 21, 2017, https://www.nytimes.com/2017/11/21/technology/uber-hack.html.

5. “Protection of Transportation Infrastructure from Cyber Attacks: A Primer,” National Academies of Sciences, Engineering, and Medicine (2016).

6. Yongdong Wu, Jian Weng, Zhe Tang, Xin Li, and Robert H. Deng, “Vulnerabilities, Attacks, and Countermeasures in Balise-Based Train Control Systems,” IEEE Transactions on Intelligent Transportation Systems 18, no. 4 (April 2017): 814-823.

7. Erica Swallow, “Anonymous Hackers Attack BART Website,” *Mashable*, August 15, 2011, https://mashable.com/2011/08/15/bart-anonymous-attack/#gZcpuZcq7sqT.

8. William Turton, “It Looks Like the San Francisco Muni Hack Was Worse Than We Thought,” *Gizmodo*, November 28, 2016, https://gizmodo.com/it-looks-like-the-san-fransisco-muni-hack-was-worse-tha-1789443579.

9. Suzanne Jacobs, “Researchers Hack Into Michigan’s Traffic Lights,” *MIT Technology Review*, August 19, 2014, https://www.technologyreview.com/s/530216/researchers-hack-into-michigans-traffic-lights/.

10. “Pro-ISIS Group Hacks NJ Transit Police Website, Publishes Personal Information: Officials,” *NBC New York*, March 29, 2016, https://www.nbcnewyork.com/news/local/Pro-ISIS-Group-Hacks-NJ-Transit-Police-Information-Publishes-List-373930871.html.

11. *NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations*, National Institute of Standards and Technology, 2013, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf; “NIST Releases Version 1.1 of its Popular Cybersecurity Framework,” National Institute of Standards and Technology, April 16, 2018, https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework.

12. “Transportation Systems Resilience: Preparation, Recovery, and Adaptation,” Washington, DC: Transportation Research Board (November 2017), http://onlinepubs.trb.org/onlinepubs/circulars/ec226.pdf.

BIBLIOGRAPHY

Dougherty, Chad, Kirk Sayre, Robert Seacord, David Svoboda, and Kazuya To-gashi. *Secure Design Patterns* (CMU/SEI-2009-TR-010). Pittsburgh, PA: Soft-ware Engineering Institute, Carnegie Mellon University, 2009. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=9115.

Isaac, Mike, Katie Benner, and Sheera Frenkel. “Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data.” *New York Times*. November 21, 2017. https://www.nytimes.com/2017/11/21/technology/uber-hack.html.

Jacobs, Suzanne. “Researchers Hack Into Michigan’s Traffic Lights,” *MIT Technology Review*. August 19, 2014. https://www.technologyreview.com/s/530216/researchers-hack-into-michigans-traffic-lights/.

Langner, Ralph. “Stuxnet: Dissecting a Cyberwarfare Weapon.” IEEE Security & Privacy 9, no. 3 (May 2011): 49-51.

“NIST Releases Version 1.1 of its Popular Cybersecurity Framework.” National Institute of Standards and Technology. April 16, 2018. https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework.

NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations. National Institute of Standards and Technology, 2013. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

“Pro-ISIS Group Hacks NJ Transit Police Website, Publishes Personal Infor-mation: Officials.” *NBC New York*. March 29, 2016. https://www.nbcnewyork.com/news/local/Pro-ISIS-Group-Hacks-NJ-Transit-Police-Information-Publishes-List-373930871.html.

“Protection of Transportation Infrastructure from Cyber Attacks: A Primer.” Na-tional Academies of Sciences, Engineering, and Medicine (2016).

Swallow, Erica. “Anonymous Hackers Attack BART Website,” *Mashable*. August 15, 2011. https://mashable.com/2011/08/15/bart-anonymous-attack/#gZcpuZcq7sqT.

“The Equifax Data Breach.” Federal Trade Commission. Accessed October 19, 2018. https://www.ftc.gov/equifax-data-breach.

“Transportation Systems Resilience: Preparation, Recovery, and Adaptation.” Washington, DC: Transportation Research Board (November 2017). http://onlinepubs.trb.org/onlinepubs/circulars/ec226.pdf.

Turton, William. “It Looks Like the San Francisco Muni Hack Was Worse Than We Thought.” *Gizmodo*. November 28, 2016. https://gizmodo.com/it-looks-like-the-san-fransisco-muni-hack-was-worse-tha-1789443579.

Wu, Yongdong, Jian Weng, Zhe Tang, Xin Li, and Robert H. Deng. “Vulnerabili-ties, Attacks, and Countermeasures in Balise-Based Train Control Systems.” IEEE Transactions on Intelligent Transportation Systems 18, no. 4 (April 2017): 814-823.

ABOUT THE AUTHOR

JACQUES REMI FRANCOEUR

Jacques Francoeur has more than 30 years of high-tech experience and is currently the Founder and CEO of Spheric Security Solutions, a Silicon Valley-based organization focusing on developing security software to support the management and communication of security. Jacques is also the co-founder and Executive Director of SecurityGenomeProject.org, a not-for-profit community-based initiative developing a Security Control Syntax Language and Security ontology for the common good of the industry. Additionally, Jacques is the Cyber Executive-in-Residence at the Lucas College & Graduate School of Business at San Jose State University and is a member of the Dean's Global Leadership Council, and as the Senior Cybersecurity Scientist at the National Transportation Security Center, Mineta Transportation Institute, he focuses on surface transportation protection from cyber threats.

Previously, Jacques was a member of Ernst & Young's Information Security Advisory team, Security Center-of-Excellence. Prior to E&Y, Jacques was Sr. Director at the Science Application International Corporation (SAIC), where he provided thought leadership in the field of identity and information assurance. Jacques was the co-founder and former Executive Director of the Bay Area CISO Council, which is a Silicon Valley member-based nonprofit organization of Chief Information Security Officers.

Jacques holds a Bachelor of Applied Science (B.A.Sc.) in Aerospace Engineering from the University of Toronto, and a Master's of Applied Science (M.A.Sc.) degree in Aerospace Engineering from the Institute for Aerospace Studies. He earned his M.B.A. from Concordia University.

PEER REVIEW

San José State University, of the California State University system, and the MTI Board of Trustees have agreed upon a peer review process required for all research published by MTI. The purpose of the review process is to ensure that the results presented are based upon a professionally acceptable research protocol.

MTI FOUNDER

Hon. Norman Y. Mineta

MTI BOARD OF TRUSTEES

Directors

Karen Philbrick, Ph.D.
Executive Director

Asha Weinstein Agrawal, Ph.D.
Education Director
National Transportation Finance Center Director

Hilary Nixon, Ph.D.
Research & Technology Transfer Director

Brian Michael Jenkins
National Transportation Security Center Director

Research Associates Policy Oversight Committee

Jan Botha, Ph.D.
Civil & Environmental Engineering
San José State University

Katherine Kao Cushing, Ph.D.
Enviromental Science
San José State University

Dave Czerwinski, Ph.D.
Marketing and Decision Science
San José State University

Frances Edwards, Ph.D.
Political Science
San José State University

Taeho Park, Ph.D.
Organization and Management
San José State University

Christa Bailey
Martin Luther King, Jr. Library
San José State University

MTI MINETA TRANSPORTATION INSTITUTE