Could Your Security Vulnerabilities Cause Network Gridlock?

A Discussion Paper for Transportation Information Technology Leaders and Executives

CGI

Experience the commitment®

THE NEED FOR SECURITY IN THE TRANSPORT ECOSYSTEM

Transportation forms an integral part of a nation's critical infrastructure. Preserving the integrity, confidentiality and availability of information and services is a leading priority for every transport organization.

It has never been more so with the advent of intelligent transport systems and services. Connected cars, connected aircraft, automated passenger journey information and self-service airports—all powered by the adoption of new technologies such as the Internet of Things—enable the tracking of passenger and freight movements.

The adoption of these services is underpinned by changes in infrastructure and the rise of new technologies, including cloud computing and shared services. These services also increase potential risks to the business.

Lloyd's Risk Index 2013 Global CXO survey[1] cites cybersecurity risks as one of the top three priorities on boardroom agendas. Failure to identify vulnerabilities and validate the effectiveness of security controls could compromise both the business and entire transport network.

The collision of physical and cyber attacks are real threats for which organizations should be prepared and ask the following questions:

- How prepared is your organization? Could it withstand a cyber attack?

- How secure are your company processes?

- How secure are your suppliers' and partners' cybersecurity defenses?

We address these and other questions as we examine the impact of the connected world and subsequent risks in the transport sector.

TRANSPORTATION TODAY

Everyone wants to feel safe when they're travelling, whether it's by road, rail, sea, air or simply on foot. A host of organizations, including governments and transport operators, are working to ensure safety—and we're right there with them.

Moving people and goods is critical to the success of any modern society and requires intelligence to be built into transport systems to minimize risk while maintaining freedom of movement. The customer experience and customer journey are fundamental to success.

At a basic level, the combination of customer experience and risk mitigation involves the use of cameras, scanners and other devices to detect and screen objects and people, while at a higher level, it also involves carrying out security evaluations, dependent upon the risk profile and risk appetite of the organization.

This paper reflects on the new realities of transportation security and risks. Incidents and events are being reported almost every day, which compel businesses to approach transport security as more than a single element of the global networks that move people and goods.

Once a routine component of modern transportation, cyber and physical security now represents a vital necessity and an urgent priority. Can you afford for your organization to be the breach in the transport ecosystem?

The aim of this paper is to provide insight and analysis for executives and decision makers around the world who understand the importance of transportation system security in today's world.

CGI in security

CGI helps clients assess cyber threats and risks, protect their business and operate with confidence. We do this with a business-focused approach to security.

CGI experts work on high-intensity engagements with military and intelligence agencies and high-profile, multi-national defense programs, defending government networks, critical infrastructure and corporate intellectual property against 43 million sophisticated attack incidents per day.

We have deployed and supported 9,000+ biometrics systems and devices at a 100+ worldwide locations, delivering more than 4 million biometrics enrolments each year for the U.S. military.

We are one of the few providers worldwide with three accredited security certification facilities—located in Canada, the U.S. and the UK—including our world-class CGI Federal Cyber Innovation Lab. Our nine Security Operations Centers continuously identify and deploy the best solutions to maintain a state-of-the-art infrastructure.

CGI in transport

CGI works with transport and logistics companies to drive efficiencies, launch innovative offerings and enhance the overall passenger experience.

We currently work with more than 200 clients providing end-to-end IT transport and logistics services, from consulting to full IT outsourcing, along with specialized IT and security services.

During our 30 years working in the sector, we have delivered the following:

- Automatic gate check-in for Lufthansa

- PCI DSS compliant service for Shell fuel cards

- Physical security at Gatwick Airport

- PCI for Transport for London

- Barclays bike hire scheme

- First biometric border control system in Europe

- Security and penetration testing for rail infrastructure owners

- Security management services for BMW

- Software that helps manage 10 airports in Portugal

CGI's transport security solutions are designed to deliver clarity to the complex task of protecting passengers, cargo and high-risk assets. We work with government, military, law enforcement and security organizations and within the aviation, maritime and rail industries to deliver the following:

- Superior passenger experience

- Increased value and efficiencies

- Protected and enhanced reputation

- Strong environmental, health and safety programs

- Compliance and governance reviews

- Examination of the security measures of organizations within their wider ecosystem

- Adoption and deployment of new technologies such as cloud and mobile apps, mindful of the security risks and business impacts

- Privacy for employee and customer data

- Review of cost of reputation and cost of money

- Examination of reputational risks and loss of customer loyalty

- Examination of financial cost of crisis management

- Threat-level assessment

- Examination of the countermeasures in place

- Recommended strategies to deal with threats

- Predictive analytics of threat vectors and countermeasures

- 24/7/365 monitoring

- Continuity of operations

Security is one of our areas of special expertise. We've carried out more than 60 percent of UK government security evaluations and provide top-level security solutions for governments and commercial organizations worldwide. In transport, we have a 30-year track record of supporting transportation organizations globally with both operational efficiencies and security improvements.

It's this kind of experience that uniquely positions us to provide safety and security solutions for the transport sector.

TRENDS AND RISK FACTORS

THE CONNECTED FUTURE OF TRAVEL AND TRANSPORT IS ALREADY HERE. ARE WE READY?

Technological advances have delivered automated self-drive cars, connected aircraft and driverless trains, but human acceptance of the reliability and legislation of these technologies delays their widespread adoption.

> Securing the supply chain and its component parts is a balancing act between cost efficiencies, new technology and compliance. CSOs, CIOs and organizations are discovering this as the threat of cyber and physical attack increases.

Improving the passenger experience should not result in lower risk factors. However, it is key to recognize that threats and risks no longer just come from individual hackers looking for vulnerable websites, backdoors or compromised software. Every day, headlines report the depths that organizations and organized crime will go to gain control of information from targeted attacks.

It is estimated that targeted attackers are, on average, able to operate for some 416 days within an organization prior to detection[2]. These targeted attacks on corporations have widespread consequences on brand, reputation and operational processes. For example, Sony lost six percent market share overnight when it suffered a security breach that resulted in the loss of sensitive customer information. The majority of global organizations are likely to have suffered some form of data loss, while data breaches have cost organizations multiple millions. Could a public transport organization recover from such a loss of reputation even if the safety of the network were preserved?

Airport scare in Los Angeles

LAX visitors were subjected to flight boards displaying, "Emergency Leave the Terminal," for five minutes. What was initially thought to be a hacking attack was actually an airline contractor who had accidently caused the override of the screens.

KLM website attacked

On April 18, 2013, KLM's website started to experience issues. Online check-in, ticket booking and other information services were non-operational. A denial-of-service attack was the cause, and it wasn't until two days later on April 20 before services began to return to normal.

2 Mandiant M-Trends 2012,: https://www.mandiant.com/news/release/ mandiant-releases-annual-threat-report-on-advanced-targeted-attacks/

Car hacking tricks revealed at Vegas hacking conference

At Defcon 21, Charlie Miller, a security engineer at Twitter, and Chris Valasek, director of security intelligence at IOActive, released their homegrown tools to hack into computerized features of a 2010 Toyota Prius and a 2010 Ford Escape. They demonstrated how easy it is to disarm the car alarm systems and control other GSM and cell-connected devices.

They were able to achieve this by a direct attack, hooking a laptop to the ECU communications network and injecting rogue signals into it. The signals included disabling the breaks while the car was in motion, jerking the steering wheel, accelerating, killing the engine, yanking the seat belt, displaying bogus speedometer and fuel gauge readings, turning on and off the car's lights, and blasting the horn.

The researchers also found a way to achieve persistent attacks by modifying the ECU firmware to send rogue signals even when they were no longer physically connected to the control units. All of these needed direct access to the vehicle to work. However, in 2011, another research group from the Center for Automotive Embedded Systems Security found that they could execute a wide range of remote attacks using the vehicles' CD or USB player, Bluetooth and cellular radio. What if these direct and remote methods were successful when combined?

WHAT DOES THIS IMPLY FOR BUSINESSES?

Organizations that are not reviewing and updating their risk profile of vulnerabilities could be subject to reputational damage or worse. They need to consider the probability and impacts of an incident or attack on their infrastructure and services. Will they be able to effectively manage and survive a crisis? Consider how many minutes it takes for the following:

- A malfunctioning baggage system to interrupt the smooth functioning of a busy international airport

- The closure of an arterial road system to create traffic jams

- An act of terrorism or violence to create a crisis situation

- The almost instantaneous loss of customer loyalty, brand and reputation

Organizations that do not assess the impact of a security incident or attack on their business, the probability that a threat will occur and the development of a mitigation strategy are putting their brand and bottom line at risk.

THE IMPACT ON THE STREET

Our transportation systems are becoming more connected. We already see widespread adoption of real-time passenger information services and mobile ticketing. Government open data initiatives are giving third-party developers access to perform data mashing, providing predictive analytics based on consumer choices and freight patterns, and much more. However, this is just the beginning of the rise in connectivity. As mobile device applications develop and the advent of the Internet of Things becomes a reality, a security strategy of isolation is no longer relevant. For example, until recently it was irrelevant and considered unnecessary to worry about the safety of allowing over-the-air updates to a vehicle.

Cars today are already becoming connected. It is predicted that by 2030 autonomous vehicles will be commonplace on our roads. With the imminent range of connected vehicles hitting production lines, transport authorities are starting to think about how our traffic management operation centers can gain greater insight into the movement of traffic and the influence of that movement. Examples include the control of vehicles to reduce emissions around a hospital where a hotspot has formed, the automatic re-direction of cars when an accident has occurred, and the automatic reduction of car speeds during periods of heavy traffic. Personalized micro-navigation requests could be directed to driver routing systems to accomplish these efforts and many more applications are in development. However, imagine the disruption if this was maliciously compromised by a disgruntled employee or a terrorist.

An intelligent connected world of transport

The infrastructure upon which we run our transportation is becoming more intelligent and connected, and signalling systems are turning digital and autonomous. This is truly where the physical and cyber worlds collide.

WHAT DOES THE FUTURE HOLD FOR US?

Rate of urbanization

Projected average rate of change in urban population size

2/3 of the planet by 2025

70% by 2050

Transport of people and goods

How things are set to change

Fewer people will maintain a car, which is currently used for only 5% of its life and stays parked for the remaining 95%

People will want to get from A to B and will worry less about the mode of getting there

Journey will become multimodal—walking, trains and car shares will all be valid options

Data, applications and personal identity will become the new tools of choice for journey

Bay Area Rapid Transit targeted by hackers

In August 2011, the Anonymous Hacking group attacked San Francisco's Bay Area Rapid Transit (BART) website, myBART.org. The attack came after BART blocked cell phone service to stop a protest the previous week. Hackers defaced the site with Anonymous logos and released personal contact information for at least 2,400 of the site's users, including names, passwords, emails, addresses and phone numbers.

Infrastructure vulnerability exposed

In 2008, a teenager derailed a tram in Łódz, Poland injuring 12 people by using a modified remote control to switch points. The ageing rail infrastructure used an infrared control system that wasn't secured in any manner.

PHYSICAL AND CYBER WORLD COLLISION

The collision of the physical and cyber worlds brings new challenges in securing the transportation sector, including the customer experience, passenger journey and freight handling. More attention on the means of attack and the consequences, as well as visionary thinking with respect to risk mitigation, is critical.

The greatest risk that transportation organizations are bracing themselves for is the combination of both physical and cyber attacks on their infrastructure. This is the highest risk factor that many are working to control within corporate risk registers. The explosion of social media applications, online technologies and self-service user terminals provide an avenue for increased risk.

The resulting risk mitigation matrix needs to take into consideration the following:

THREATS AND MOTIVATIONS

- **Deliberate and planned**: protester, terrorist, criminal, disgruntled passenger, employee or third party
- **Deliberate and spontaneous**: opportunistic criminal, disgruntled passenger, ex-employee or third party
- **Malicious and non-specific**: malware, hacking, spoofing
- **Malicious and specific**: targeted attack on business, industry or ecosystem
- **Environmental**: weather, power loss, act of God
- **Accidental**: unintended consequences

MEANS OF ATTACK

- Physical access
- Interfaces
- Cyber attacks: Internet-borne malware
- Wi-fi
- Denial of service
- Lock out

POTENTIAL IMPACT

- Impact on information, confidentiality, integrity or availability

- Loss of information and communications technology (ICT)

- Interrupted operations resulting in delays, cancellations

- Impairment of passenger/freight experience

- Damage to reputation and brand

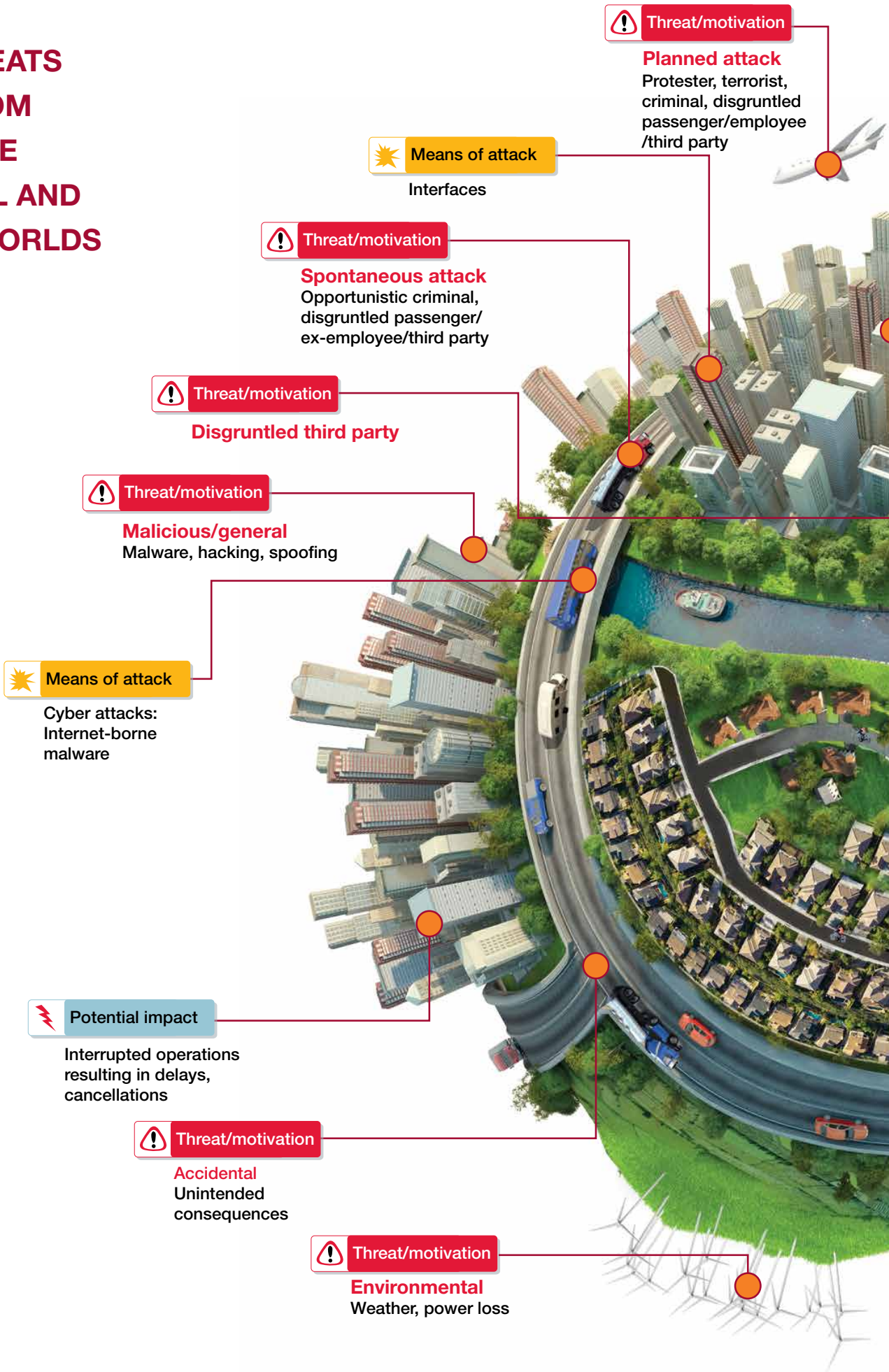- Incorrect freight/passengers, transport at wrong destinations causing security breaches

Crisis management scenarios need to consider not only attacks to the direct organizational infrastructure but also to the wider transportation system. Incidents such as volcanic ash clouds, fires on airport runways and high speed passenger train crashes demonstrate the need for immediate and effective handling.
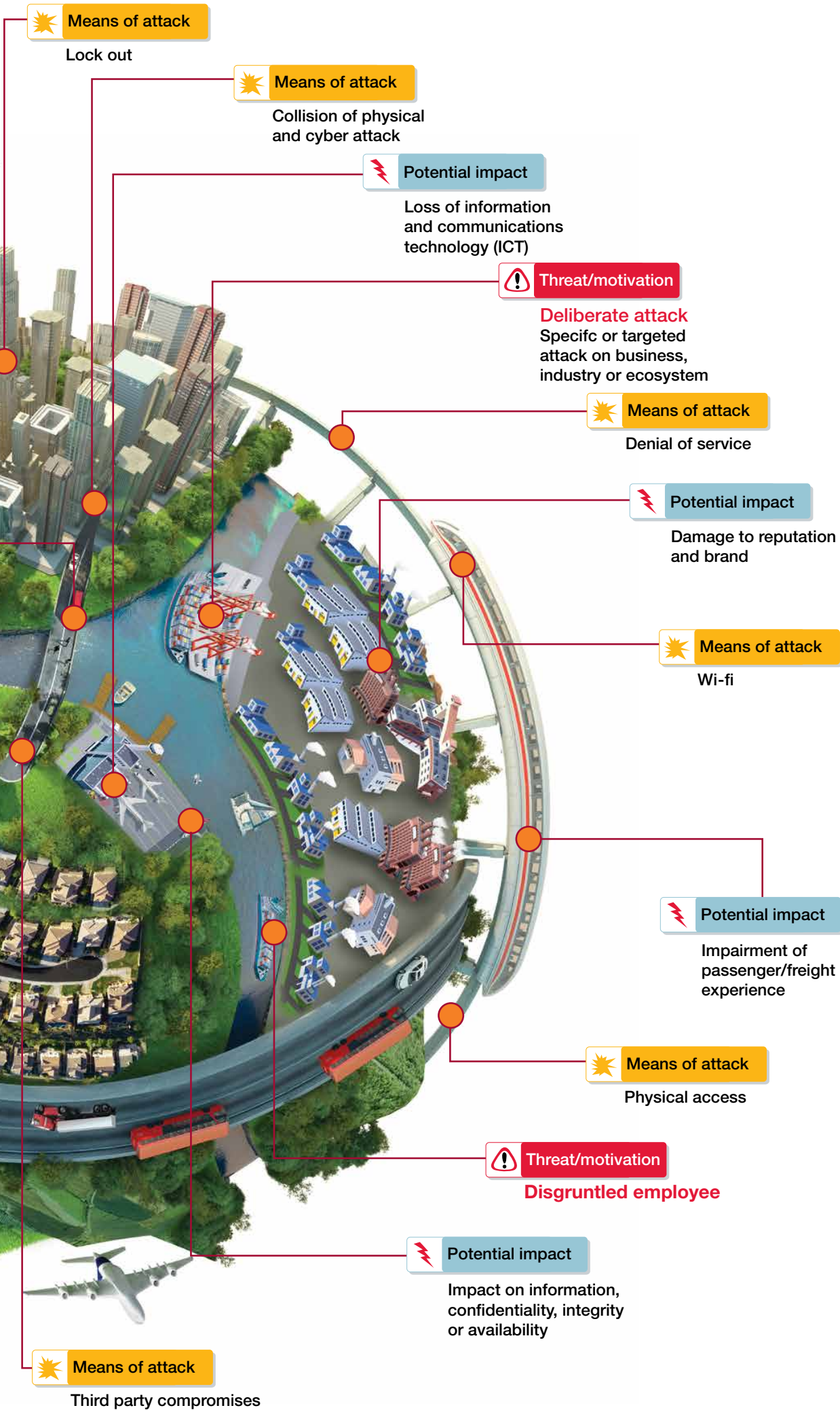
But when does an incident turn into a crisis? And how do organizations manage events both within and out of their sphere of control? As we highlighted earlier, Mandiant[3] has reported that hackers could be within an organization's infrastructure for up to 416 days before detection. To mitigate risks, this needs to be reduced to almost instant recognition. If you secure your environment how can you be assured that your competitors and third party suppliers have also secured their vulnerabilities?

3 Mandiant M-Trends 2012, https://www.mandiant.com/news/release/mandiant-releases-annual-threat-report-on-advanced-targeted-attacks/

THE THREATS THAT LOOM WHEN THE PHYSICAL AND CYBER WORLDS COLLIDE

⚠️ **Threat/motivation**

Planned attack
Protester, terrorist, criminal, disgruntled passenger/employee /third party

💥 **Means of attack**

Interfaces

⚠️ **Threat/motivation**

Spontaneous attack
Opportunistic criminal, disgruntled passenger/ ex-employee/third party

⚠️ **Threat/motivation**

Disgruntled third party

⚠️ **Threat/motivation**

Malicious/general
Malware, hacking, spoofing

💥 **Means of attack**

Cyber attacks: Internet-borne malware

⚡ **Potential impact**

Interrupted operations resulting in delays, cancellations

⚠️ **Threat/motivation**

Accidental
Unintended consequences

⚠️ **Threat/motivation**

Environmental
Weather, power loss

Means of attack

Lock out

Means of attack

Collision of physical and cyber attack

Potential impact

Loss of information and communications technology (ICT)

Threat/motivation

Deliberate attack
Specifc or targeted attack on business, industry or ecosystem

Means of attack

Denial of service

Potential impact

Damage to reputation and brand

Means of attack

Wi-fi

Potential impact

Impairment of passenger/freight experience

Means of attack

Physical access

Threat/motivation

Disgruntled employee

Potential impact

Impact on information, confidentiality, integrity or availability

Means of attack

Third party compromises

The world's largest ITS project

Saudi Arabia has a population of 27 million and suffers 18 fatal accidents daily, five times the per capita rate in Europe.

The Automated Traffic Violations Administering and Monitoring (ATVAM) program covers all eight of the kingdom's major cities and addresses the need to improve road safety, law enforcement and security, as well as reduce congestion through better traffic management.

The kingdom has been divided into three regions overseen by CGI.

The program provides several thousand roadside systems split between number plate detectors, intelligent surveillance, and fixed and mobile speed and red light cameras. A dozen command and control centers bring together the security and traffic management functions and attention to process violations.

This is a perfect example of the ITS industry demonstrating that it can rise to the challenge of coping with the harsh and unpredictable conditions in Saudi Arabia to make its systems work there as effectively as they do elsewhere in the world and to raise the bar globally in terms of true system integration.

PREVENTION - SECURING AND ASSURING

Risk mitigation provides assurance for today's risks, as well as tomorrow's. From connected cars to last-mile parcel delivery, transport and logistics systems need to be robust and defended.

In engagements with organizations such as British Airways, a large UK rail operator, and others, CGI has identified the core components of risk mitigation to ensure every area is tested for vulnerabilities. In addition, we have undertaken cyber risk assessments using cyber intelligence gleaned from our global Security Operation Centers and applied it to the external cyber vulnerabilities of each organization.

Our methodology and approach has been developed over more than 30 years. Our specialist Penetration Testing Team founded the CESG CHECK scheme, and we currently have a "green light: status." The team comprises highly skilled security consultants who specialize in penetration/vulnerability testing and includes CESG CHECK approved team leaders and team members.

OUR PRIMARY OBJECTIVES FOR SECURITY ASSURANCE:

- To demonstrate to the highest level of assurance possible that a system is either susceptible or not susceptible to particular security weaknesses

- To provide clear recommendations for vulnerability mitigation that are straightforward to implement and tailored to the system's requirements

- To validate the solution and identify the weakest security link

- To ensure the security of the underlying software using CGI's SilverKite solution

CGI was selected for a multi-award, indefinite delivery/indefinite quantity (ID/IQ) Technical, Acquisition and Business Support Services (TABSS) contract with the Department of Homeland Security (DHS).

TABSS provides support for the planning and administration of programs, projects and major acquisitions that are key to advancing the DHS's goals and securing the nation.

CGI will compete for task orders to provide mission-critical engineering, program management and technical services to support the entire acquisition lifecycle—from research and development, to production and deployment, to operations, upgrade and disposal of essential DHS programs and assets. Our domain expertise and next-generation solutions enhance DHS's mission capability and improve cost effectiveness across the agency.

NS gets control over its entire passenger information chain

CGI helped Dutch railway operator, NS, orchestrate its efforts to proactively manage its information chain. By doing this, it was able to resolve issues before they turn into problems, have one common image on the health of the entire chain, zoom in on specific elements in the chain, and solve incidents and problems faster.

BMW implements one of Europe's largest identity management systems—among the top 50 systems of its kind worldwide

More than 1,000 of BMW's applications supporting a user base of 280,000 employees, dealers and suppliers were based on multiple platforms and used different processes and systems. Over time and with increasing business demands these systems became unsustainably complex with correspondingly high support and maintenance costs. BMW looked to CGI to help meet its evolving security needs and comply with changes in international law.

We designed and developed BMW's new identity management system (IdAS), which integrates formerly disparate management and provisioning processes and meets BMW's need for flexibility, security and speed. IdAS was successfully launched in 2009. BMW customers now get more information from dealers as the dealers have direct access to BMW's information systems.

TRAVEL, TRANSPORT AND SECURITY UNDERSTANDING

TRUSTED PROJECT RESOURCES AND PROVEN EXPERIENCE WITHIN THE TRANSPORT AND LOGISTICS SECTOR

We have worked in the transport and logistics sectors for more than three decades with organizations that include major airports such as London Heathrow, Gatwick Airport, Amsterdam Airport Schiphol and Aeroportos de Portugal. Other key clients with whom we have a close association in the aviation sector include CAA and airlines such as Air Canada, Lufthansa, Air France/KLM and Finnair.

In rail, we work with organizations such as Via Rail, ProRail, Network Rail, Queensland Rail, Deutsche Bahn, and STM and AMT in Montreal. We provide services to car manufacturers such as BMW, KIA, Ford, Toyota, Jaguar and Land Rover, and aircraft manufacturers like Rolls Royce, Bombardier and Airbus. We work with the transport ministries of national governments, such as those in Sweden, Finland and the Netherlands, and transport authorities such as Transport for London, Transport for Greater Manchester, Translink in Vancouver, and calTrans.

LEADING SECURITY PARTNER

Our decades of travel and transport knowledge include vast security expertise, enabling us to deliver a world-leading security capability. We meet the security needs of governments and blue chip organizations across the globe. For more than three decades, we have helped our clients to operate securely across the private and public sectors globally, with a business-focused approach to security. Our integrated team of more than 1,200 security professionals serve clients locally while leveraging our vast global capabilities.

Our solutions integrate consultancy, systems integration and managed services to ensure that the critical people, business processes and technology aspects are addressed. Through this, we have gained a unique understanding of how the complex security needs of our clients can be met while maintaining their business agility, improving their operational excellence, and increasing the trust of their own customers, suppliers, stakeholders and employees.

Internationally, our security teams support many of the world's leading organizations including Barclaycard, Bombardier, BMW, Carrefour, Czech Post, Daimler Benz, Department of Defense, EADS, Eon, European Space Agency, National Audit Office, Network Rail, Philips, Sagem, SAS, Scania, Shell, SNCF, Scottish and Southern Electric, T-Mobile and Transport for London.

We support and secure many critical national infrastructures. Our global methodology supports organizations like Shell as it tackles information risk management for today and tomorrow's technology challenges.

SUMMARY AND CONCLUSION

Transport systems are attractive targets for individuals seeking to inflict major disruption and economic damage. They are inherently vulnerable to attack because they are open systems that serve large numbers of people at predictable times in predictable places.

CGI is constantly thinking ahead to the next level of protection. For example, we help secure the Galileo Satellite Navigation Program. We're providing the security and key management facilities to Galileo's ground control and ground mission segments.

We're also addressing the thorny issue of achieving a balance between rigorous security checks, passenger convenience and speed of boarding. We've pioneered automated and biometric border management, with automatic barriers linked to advanced biometric readers and smart cards. This enables travellers to move quickly and comfortably through airports or between countries, without compromising security.

Biometrics is one of our core capabilities. We're one of the world's most experienced biometric implementers. Our systems are already used at football stadiums, shopping malls, and many other places with a high concentration of people or high security demands.

Major rail operator gets safer

We enhanced a major rail operator's security in four phases:

- Developed a functional view or "rich picture" that included the as-is and to-be status of the organization

- Created a cyber threat profile from internal and external data sources

- Provided a detailed analysis in specific areas, i.e., security policy, telecoms, risk management, security operations, SCADA, signaling systems and major projects and systems

- Produced a written report and options paper that laid out the options for the future expansion of the organizational's cyber defense. The report was disseminated to the information security team and key stakeholders. A formal review and feedback process was initiated. New information was provided and changes were agreed and implemented in the new version of the report.

CGI

cgi.com/cyber

With 68,000 professionals operating in 400 offices in 40 countries, CGI fosters local accountability for client success while bringing global delivery capabilities to clients' front doors. Founded in 1976, CGI applies a disciplined delivery approach that has achieved an industry-leading track record of on-time, on-budget projects. Our high-quality business consulting, systems integration and outsourcing services help clients leverage current investments while adopting new technology and business strategies that achieve top and bottom line results. As a demonstration of our commitment, our average client satisfaction score for the past 10 years has measured consistently higher than 9 out of 10.