APMA Cybersecurity Committee | CyberKit 1.0

APMA
LEAD. REACH. CONNECT.

Fall 2019

"The methods that will most effectively minimize the ability of intruders to compromise information security are comprehensive user training and education. Enacting policies and procedures simply won't suffice.

Even with oversight the policies and procedures may not be effective: my access to Motorola, Nokia, ATT, Sun depended upon the willingness of people to bypass policies and procedures that were in place for years before I compromised them successfully."

Kevin Mitnick – World's most famous hacker of his time

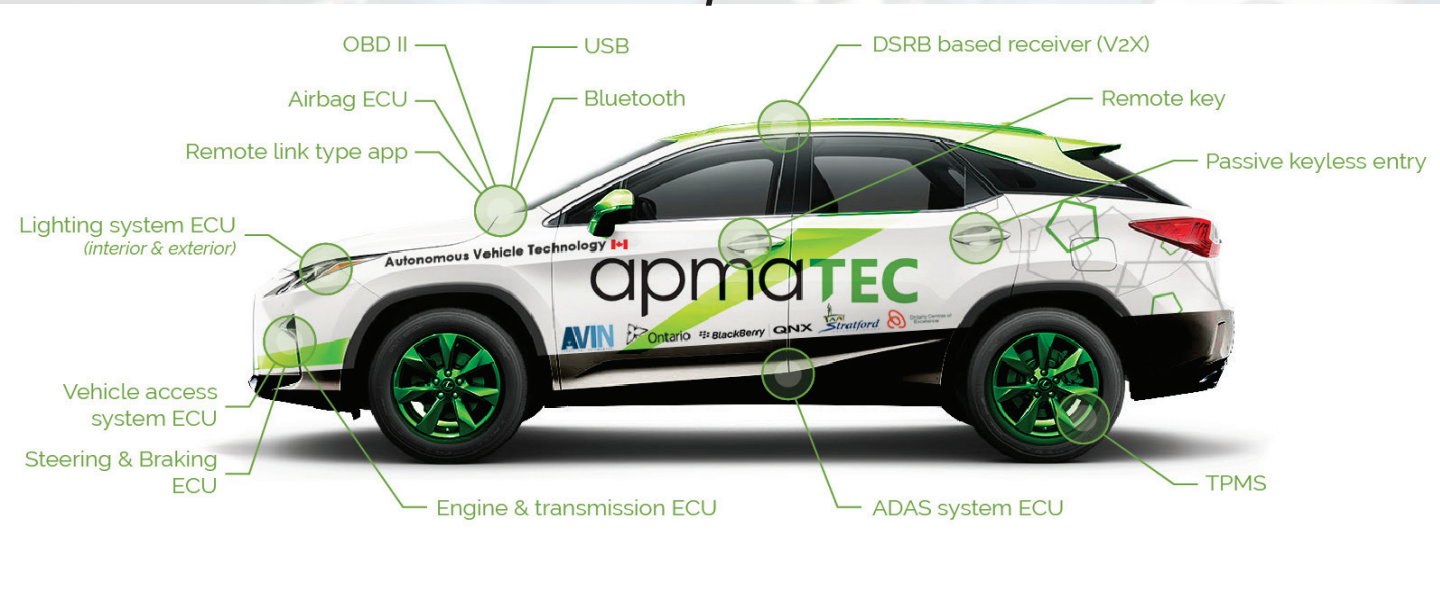
Table of Contents

1.0 - Introduction to the Cyber Security Committee

Cybersecurity in the Automotive & Manufacturing Sectors is becoming increasingly critical in Industry 4.0 as everything within the industrial ecosystem becomes more connected to the internet and other technical systems and industries. The electronics in modern vehicles are built from components supplied by multitudes of vendors from numerous suppliers who have few to no common cybersecurity standards to adhere to, and few privacy or security provisions in their manufacturing facilities. This makes the current supply chain for vehicles extremely porous in respect to cybersecurity. Every possible vendor and all electronic components are a potential point of vulnerability.

Distributed Denial of Service (DDOS) attacks, Ransomware, Spoofing, Phishing, Smishing, Spear Phishing, Whaling attacks, Malware outbreaks, Website or domain compromises or takeovers, Insider threats, Botnets, Physical manipulation/damage/theft/loss, Data breaches/information leakage, and Cyber extortion are costing the global business sector billions of dollars annually. Emails creating tax fraud, fake invoices, sextortion scams, or traditional Trojan malware are making their way into our offices and manufacturing facilities.

Potential Attack Points of a Connected Vehicle



Today's vehicles consist of multiple computers, called electronic control units (ECUs) that control door locks, windows, engine, transmission, lights, and many other components. The ECUs communicate with each other over a vehicle network. These networks can be accessed through the on-board diagnostic (OBD II) port which is the access point for a vehicle's self-diagnostic and reporting capability. The controller Area Network (CAN) is the most widely used signaling protocol, allowing microcontrollers and devices to communicate and send critical data to each other.

At the beginning of 2019, the Automotive Parts Manufacturers' Association took the important step of creating a Cyber Security Committee (CSC). Further to the obvious goal of making our parts suppliers cyber secure, the secondary goal of the CSC is to make companies more competitive. To the end, the APMA has brought together globally-recognized leaders in cybersecurity and privacy organizations from the auto sector, quantum computing, blockchain, academia, and the insurance industry to be part of the CSC. The current gaps and discrepancies within the automotive supply chain could lead to compromised software and hardware finding its way through to OEM vehicles. This needs to be addressed.

This document has been developed by the CSC. Its goal is to support the safety, privacy, and security culture of the Canadian automotive industry by providing organizations with resources to help them understand and implement security best practices and to develop a secure supply chain and development process. The objectives of this document are:

- To provide expertise in determining and implementing best practices for securing products manufactured within a facility and also for securing the facilities themselves, their employees, and all Internet-of-Things (IOT) equipment
- To provide companies with guidelines for communicating to shareholders, regulatory authorities, and employees in the case of a security incident
- To support understanding of cybersecurity insurance requirements
- To provide cybersecurity education for employees and executives
- To aid companies and organizations in understanding the impact of cybersecurity threats and the associated risks to the company's bottom line.

2.0 -The APMA Cyber Kit 1.0

This document has been developed as a guidance document for organizations in the Automotive Sector that have recently started their Cybersecurity journey and those that a re yet to begin. This CyberKit 1.0 will provide the means to develop a holistic Cybersecurity Program which is robust, secure, practical, and effective. It will also help Organizations to understand its critical assets and the risks associated with them. Based on this knowledge, the Organization can develop relevant and effective Cybersecurity Controls to ensure that its assets are protected.

This toolkit focuses on all aspects of a Cybersecurity program including People, Processes, and Technology. Today, there is great reliance on technology alone to keep adversaries and hackers from accessing an organization's data. However, as we are starting to see more and more, technology alone cannot ensure protection of data assets. Therefore, the APMA CyberKit 1.0 provides Cybersecurity professionals in the automotive sector with an expanded arsenal that extends far beyond reliance on the latest technical products alone.

The Intended Audience

This toolkit is intended for professionals involved in managing and delivering a Cybersecurity Program at any Automotive Organization. Having this role is extremely challenging as Cyber Governance managers needs to be to be as agile, multifunctional, flexible, and dynamic as the threats they now face. To meet that challenge, they must have diverse knowledge to perform many different activities, respond to new threats and shift priorities to meet the challenge of the day. Therefore, this toolkit can help individuals who are in the below-mentioned roles.

- Chief Executive Officers (CEO)
- Chief Financial Officers (CFO)
- Chief Operating Officers (COO)
- Chief Information Officers (CIO)
- Chief Information Security Officers (CISO)
- Information Technology Manager
- Vice President (Information Technology)
- Information Security Manager
- Cybersecurity Manager
- IT Security Manager

Cyberkit Structure

This Cyberkit has been designed to provide step-by-step guidance for Cyber Managers and has been broken down into the following areas:

- Cybersecurity Program Development
- Gap Analysis / Threat & Risk Assessment
- Cyber Governance Framework
- Cyber Education & Awareness
- Cybersecurity Insurance
- Risk Mitigation
    - Incident Response Planning
    - Penetration Testing / Vulnerability Analysis
    - Continuous Monitoring
- Supply Chain / 3rd Party Cyber Assessment

Benefits of the APMA CyberKit 1.0

The aim of the *APMA CyberKit 1.0* is to provide a how-to guide for its members to implement Cyber Governance principles. Benefits of utilizing the APMA CyberKit include:

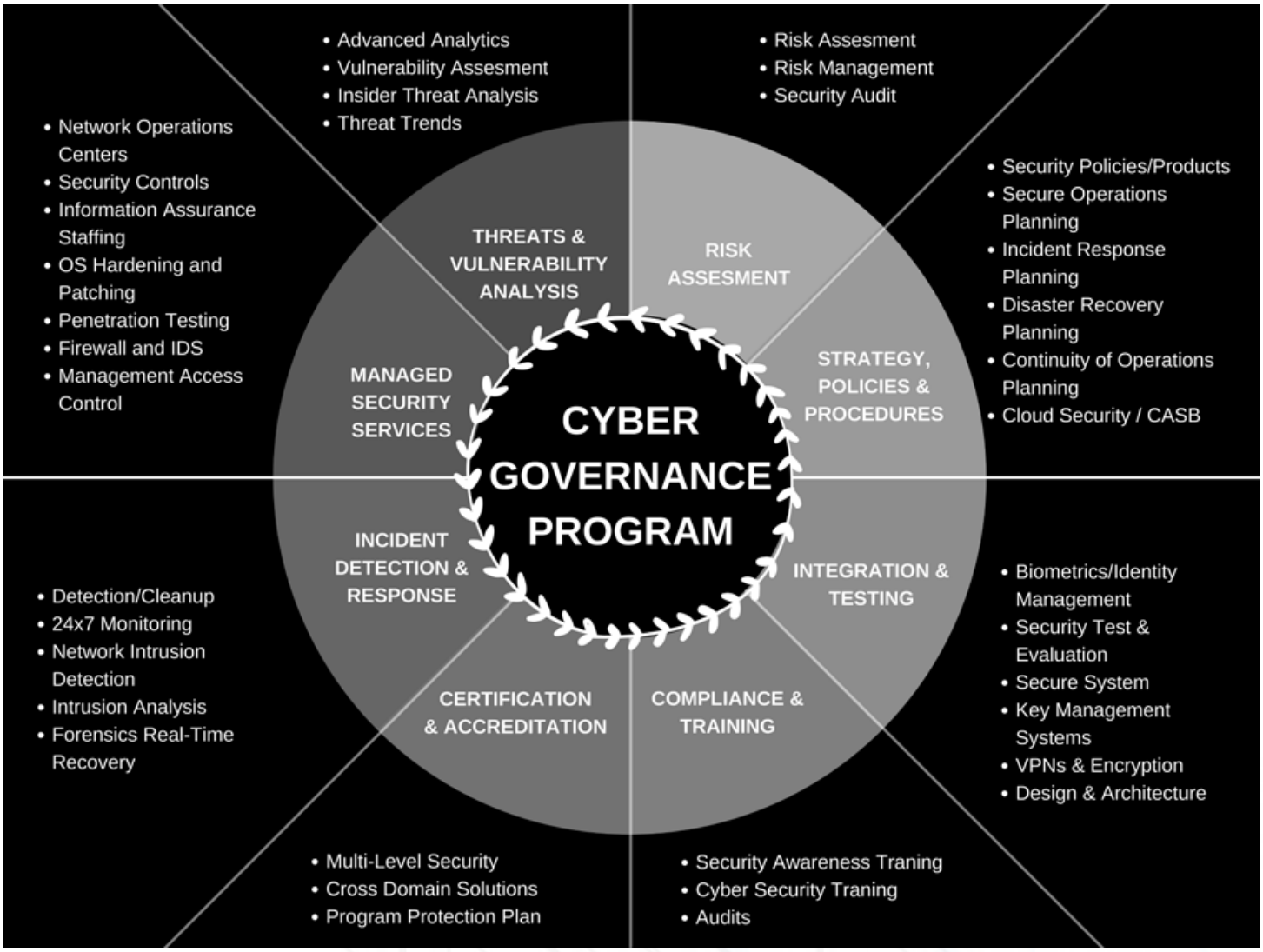
- Increased reliability and security of systems and information
- Improved customer and business partner confidence
- Increased business resilience
- Alignment with customer requirements (present and future)
- Improved management processes and integration with corporate risk strategies
- Assessing the potential risks to your business and identifying areas that are vulnerable
- Protecting information from getting into unauthorizeed hands
- Ensuring information is accurate and can only be modified by authorized users
- Mitigating the impact of a breach, including Incident Reporting & Communication

"It's Time for an Automotive Cybersecurity Wake-Up Call"

(securityintelligence.com/march 2019 by Mark Stone)

3.0 - Cyber Governance Development Program

Successful, well-managed companies conduct themselves based on their corporate governance. This is especially true for the Automotive Sector which has Corporate Governance defined from Original Equipment Manufacturers (OEMs) to other parts of the supply chain including Tier 1 & 2 Suppliers as well as dealer & distributor networks. Corporate Governance is a set of rules, policies, processes, practices and procedures. This structure of Corporate governance is critical for ensuring that the needs of the company's many stakeholders are met. These stakeholders include investors, shareholders, employees, customers, partners, and the community - each of which have different needs and interests that must be protected using Corporate Governance.



The above figure shows the components that are part of any holistic Corporate Governance framework in an organization. As you can see, there are a myriad of activities that need to be carried out for effective Corporate Governance. However, any Corporate Governance frameworks must follow certain basic principles.

These principles include:

- Clearly Defined Strategic Objectives
- Organizational Discipline through an established Governance Framework
- Effective Risk Management
- Protecting the interests of the Employee & the Customer
- Ownership, Accountability & Transparency
- Continuous Improvement

As organizations in the automotive sector increase their reliance on technology (leading to increasing Cyber Threats that can impact their operations), there is a critical need to include a Cyber Governance program as part of all Corporate Governance initiatives. An effective Cyber Governance Program defines ownership of all aspects of an organization's Cyber initiatives and defines the structure used to implement and operate the program. It encourages and promotes accountability at the board level which is essential in the highly regulated automotive sector. The Program provides a holistic view into the framework of standards, processes and activities that contribute to securing an organization against cyber risk.

A complete Cyber Governance Program also facilitates reporting to outside stakeholders (e.g. OEMs, industry certification bodies, or government agencies) on the cyber initiatives carried out by the organization. It also safeguards the board's liability, in the event that a security incident occurs, as they would be able to show reasonable efforts were taken to safeguard the organization against security risks.

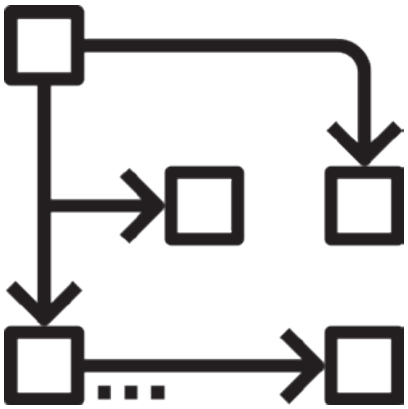
The key components of establishing a Cyber Governance Program include:

- Establishment of a Cyber Governance Strategy
- Changing the culture of the organization to be more Cybersecurity Aware
- The establishment of an Organizational structure to lead and implement Cybersecurity initiatives in the organization

These three components for developing a complete Cyber Governance Program are discussed in the next few pages.

Cyber Governance Strategy

The Oxford dictionary defines the term "Strategy" as "A plan of action designed to achieve a long-term or overall aim", while the Business Dictionary defines "Strategy" as "a method or plan chosen to bring about a desired future, such as achievement of a goal or solution to a problem."



Icon made by Becris on www.flaticon.com

The first step to developing a Cyber Governance strategy involves a discussion at the highest level of the organization wherein a need is acknowledged for such a strategy within the organization. In other words, buy-in on the importance on a Cyber Governance strategy must come from the top.

A Cyber Governance Strategy is needed to support the Governance Program. It should be aligned with the strategy of the organization as a whole and seen as critically important to sustain the competitive advantage of the organization's business in the automotive sector. A Cyber Governance Strategy centered around awareness and resilience should be a priority for everyone in the organization and be made part of the prevailing corporate culture.

The Cyber Governance Strategy is in many ways an organizational vision / mission statement that declares the objectives of the organization and the importance of Cybersecurity in achieving those objectives. Thus, the Cybersecurity Strategy must set the direction for the entire organization's Cybersecurity efforts. In this process, a few key questions must be answered in the Cybersecurity Strategy:

- What is the Organizational Vision with regards to Cybersecurity?
- What are the business drivers for enabling Cybersecurity in the organization?
- What does a SWOT* analysis of your organization say about your current situation?

  Strengths – What are you doing right?
  Weaknesses – What are you doing wrong?
  Opportunities – How will a better Cybersecurity program allow you to expand your competitivness?
  Threats – Where are you most exposed?

- Can the Organization leverage external factors to excel in business by enabling Cybersecurity Best practices?

- What are the Critical Success Factors needed for the Organization to thrive in enabling a successful Cybersecurity Program?

- Which Cyber Governance Frameworks & Standards should be implemented by the Organization?

**The Organization can carry out a SWOT (Strengths-Weaknesses-Opportunities-Threats) Analysis to answer many of the above questions. This was a method that was designed by Albert Humphrey for the Stanford Research Institute in the 1960s and can easily be adapted to explore the Cybersecurity Strengths, Weaknesses, Threats & Opportunities for the Automotive Organization.*

Cybersecurity Culture Change

Changing corporate culture to better embrace Cybersecurity in an Organization is critical for the long-term success of the Cybersecurity Strategy. Cybersecurity as an idea must be "baked in" to the culture, attitude and attention of ALL the stakeholders, including management, employees, shareholders, suppliers and customers. Building a Cybersecurity Strategic plan is the first step in changing the culture of the Organization with regards to Cybersecurity. If this is not done properly, the Organization will not meet the mission objectives laid out in the Cybersecurity Strategy.

Any change in the Cyber Security culture of the Organization should (as mentioned above) begin at the highest level of the Organization and propagate in a top-down manner. The Board is ultimately responsible for Cybersecurity efforts in the Organization and thus, sets the agenda that every stakeholder must follow. It is essential that cybersecurity remains on every agenda throughout the organization. Corporate Cybersecurity Policies and objectives must be clearly defined and adherence to them must be on every performance plan and annual appraisal. The aim of a properly designed Cybersecurity Program is to produce a culture where everyone in the organization recognizes and executes their role in protecting the confidentiality, integrity and availability of the organization's information.

However, building a Cybersecurity Culture is more than simply encouraging/training/mandating employees to following a finite list of Cybersecurity Policies and Procedures. An organization will have a mature Cybersecurity culture only when everyone truly "owns" the idea of Cybersecurity and begin to see it as their own personal responsibility.

Some principles for cultivating a Cybersecurity Cultural change in the organization are:

- Cybersecurity is a responsibility that everyone shares
- The critical importance of all members of the Organization being cyber-aware
- Secure development processes are critical to the Organization's Cybersecurity Profile
- The reward structure of the organization should incentivize Cybersecurity Best Practices
- Develop a Cybersecurity Community in the Organization
- Cybersecurity should be engaging and fun

A recent survey of auto manufacturers found 62% of respondents think it is likely or very likely that malicious attacks on their software or components will occur within the next 12 months. Even more concerning, 30% of survey respondents said they do not have an established product cybersecurity program or team.

Establishment of a Cybersecurity Structure in the Organization

Any Cybersecurity incident has the potential for serious consequences. As an example, a Cybersecurity breach might not only drive down revenue by making technology systems unavailable to customers, it could also affect the reputation of the company. Depending on the nature of the attack, existing and potential customers might turn to competitors as they no longer trust that organization with their confidential data. Therefore, it's critical that a company's Cybersecurity culture be wholistic and adopted from the top-down, with clear guidelines of processes and responsibility flow-charts.

Given the above, it is critical that an Organizational Structure for Cybersecurity be written and that all Cybersecurity responsibilities in the event of an incident are clearly defined. Usually, this structure is either Cybersecurity reporting to the Chief Information Officer (CIO) or as a separate Governance, Risk & Compliance (GRC) function directly to the CEO. While there may be other options and considerations for the organizational hierarchy of the Cybersecurity role, it is recommended by the APMA CSC that a Chief Information Security Officer (CISO) function be established and the person in that role be givin the ability to report directly to the CEO instead of through the CIO. One reason for supporting this structure is the fact that Technology and Cybersecurity have different priorities and objectives. Technology individuals usually are in a hurry to meet deadlines for enabling the business while Cybersecurity often insists on implementing project security, even if that means some delays. Another important reason is to provide segregation of duties. Cybersecurity is often auditing the work of Technology. Having them in the same reporting chain can make Compliance an issue.

Below are the Best Practices for establishing a Cybersecurity Structure in an Automotive Organization

- Establish the Chief Information Security Officer (CISO) role and assign ownership and accountability of the Cybersecurity Program to them

- Establish a Cybersecurity Leadership Committee that defines the relationships between the CISO and other C-level executives such as CEO/COO/CFO/CIO and enables input from all senior executives to the Cybersecurity initiatives in the organization

- Define Governance, Risk & Compliance roles under the CISO that evaluates the risk appetite of the organization and enable a Governance Framework

- Define Cybersecurity Operations roles under the CISO that actively manages the threats to the organization on a continuous basis

- Define Cybersecurity Training & Awareness roles under the CISO for ensuring a culture change with regards to Cybersecurity in the organization

- Define 3rd Party Cybersecurity Management as a separate role under the CISO for ensuring compliance of vendors to the Cybersecurity needs of the organization

- Ensure that HR is fully involved in enabling the Cybersecurity Structure and has talent management in this field as a top priority

Resources

Below are additional resources for enabling a holistic and effective Cyber Governance Program

AUTO ISAC	Auto ISAC has a detailed best practice guide on Governance for the Automotive Organization	https://www.automotiveisac.com/best-practices/
Automotive Cyber Governance	Free video on threats faced by the automotive sector and how to build an effective cyber governance program.	https://www.automotivecybergovernance.com/

Sources:

https://www.oxfordreference.com/view/10.1093/oi/authority.20110803100536243

http://www.businessdictionary.com/definition/strategy.html

4.0 - Gap Analysis / Threat & Risk Assessment

One of the most important responsibilities of the Cybersecurity team is to carry out a Gap Analysis or a Threat & Risk Assessment (depending on the level of detail required to analyze the risk to the organization). Gap Analysis are done at a high-level and provide a comparison of the Organization's security program with Cybersecurity best practices. A Threat & Risk Assessment is more detailed and follows defined methodologies to explore the Risk Impact to each asset owned by the Organization and ultimately monetize the impact of various threats to your organization. This enables the organization to develop an appropriate strategy for handling the various aspects of Risk Management such as: Risk Transfer, Risk Mitigation, Risk Avoidance or Risk Acceptance.

Gap Analysis

- Choose the appropriate Governance Framework to carry out the Gap Analysis

- Evaluate Policies, Processes & Procedures in the organization against the best practices of the chosen Governance Framework

- Evaluate the technology used in the Organization against the controls defined in the Governance framework

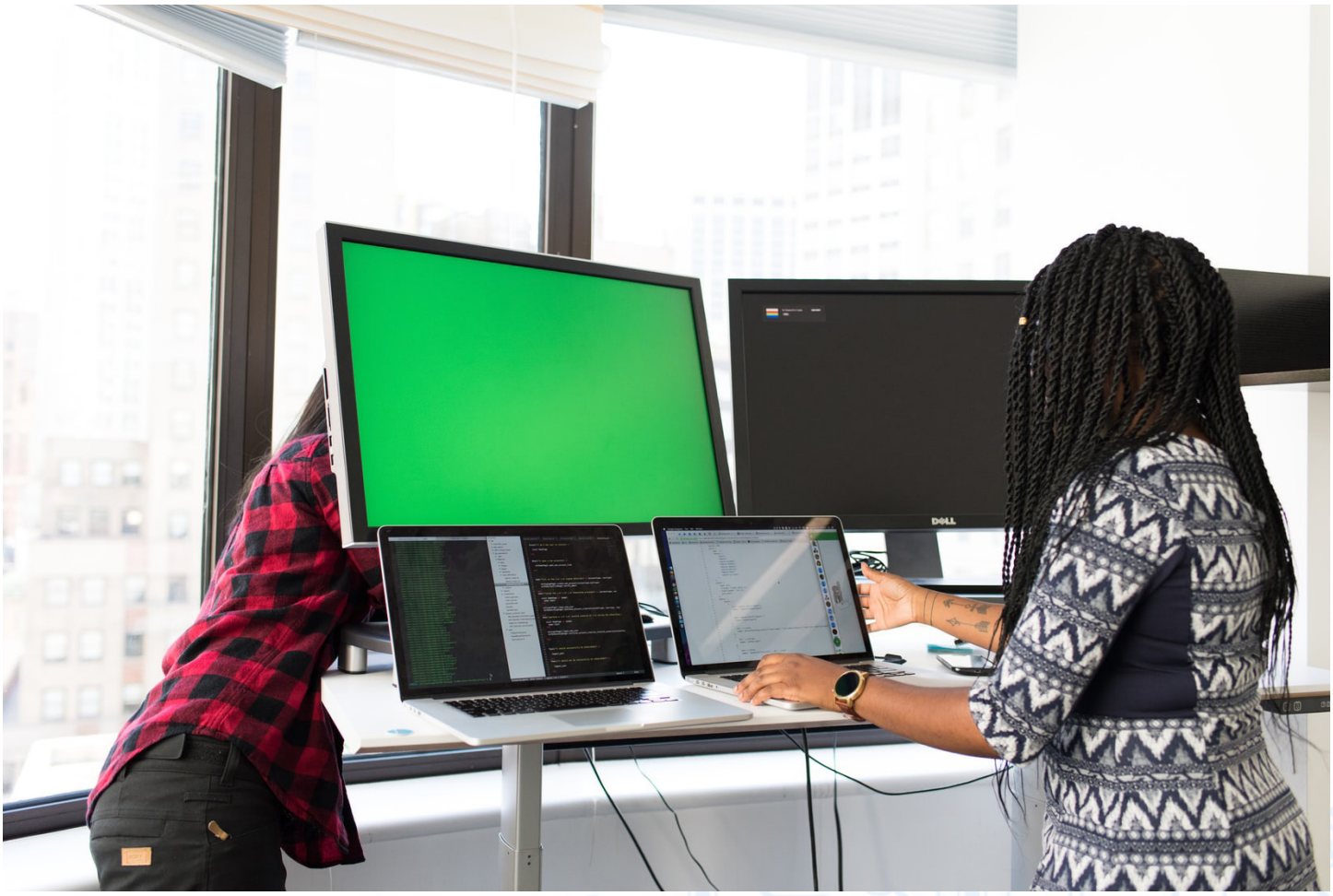
- Analyze the data and develop a roadmap for short-, mid- and long-term enhancement of Cybersecurity in the Organization

Threat Agency Risk Assessment (TARA)

As mentioned earlier, TARAs are conducted based on specified methodologies that determine the impact of Risks that have been identified to the organization. In Canada, one of the most common TARA methodologies is the Harmonized Threat and Risk Assessment (HTRA). Other examples of common TARA methodologies include OCTAVE and NIST RMF.

Regional Resilience Assessment Program (RRAP)

An example of an excellent initiative by the Canadian Federal Government is the Regional Resilience Assessment Program (RRAP) and Critical Infrastructure Assessments Tools, available through the Ministry of Public Safety Canada. The RRAP uses on-site assessments to help organizations measure and improve their resilience by identifying dependencies and vulnerabilities and providing owners/operators with ways to mitigate threats and improve their ability to respond and recover from cyber disruptions. The service is free of charge (https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-rrap-en.aspx).



Resources

Below are additional resources for enabling a Gap Analysis / Threat & Risk Assessments

Harmonized Risk and Threat Assessment (HTRA)	Harmonized Threat and Risk Assessment (HTRA). This is a methodology issued as an unclassified publication, under the authority of the Chief, Communications Security Establishment (CSE) and the Commissioner, Royal Canadian Mounted Police (RCMP).	https://www.cyber.gc.ca/en/guidance/harmonized-tra-methodology-tra-1
NIST Risk Management Approach		https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview
OCTAVE Risk Management Approach		https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=5645
RRAP Program from Public Safety Canada		https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crt-cl-nfrstrtr-rrap-en.aspx
Auto ISAC best practice guide on Risk Assessment		https://www.automotiveisac.com/best-practices/

5.0 - Cyber Governance Frameworks

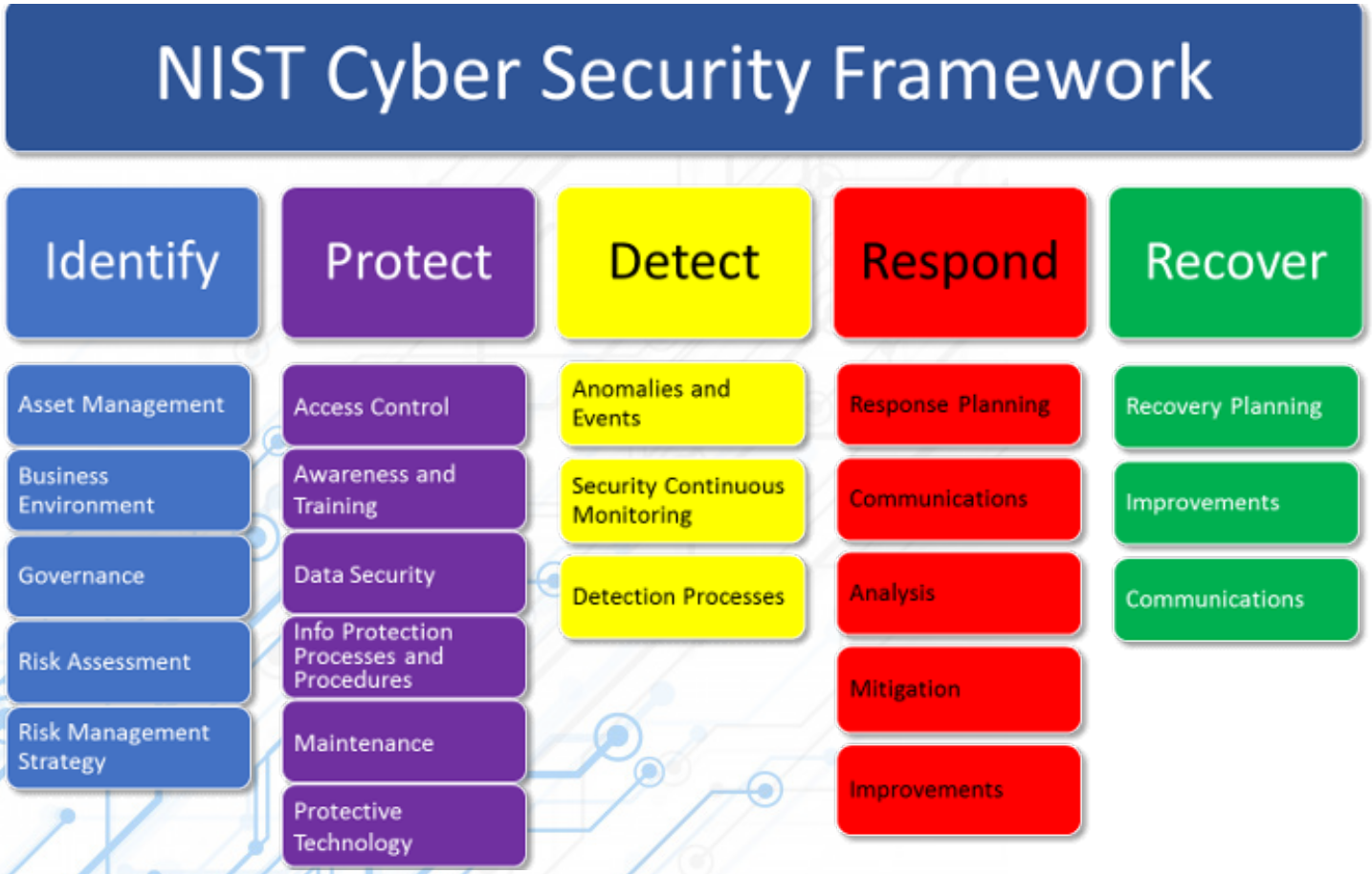
The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) was established in 2013 as a result of the Improving Critical Infrastructure Cybersecurity Executive Order issued by United States President Barack Obama. The NIST CSF aims that organizations build their Cybersecurity Organizations based on the voluntary development of a risk-based cybersecurity framework. The NIST CSF has the following principles:

- Developing critical infrastructure cybersecurity
- Applying principles and best practices of risk management
- Improving the security and resilience of critical infrastructure

The Framework provides a common taxonomy and mechanism for Organizations to:

- Describe their current cybersecurity posture
- Describe their target state for cybersecurity
- Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
- Assess progress toward the target state
- Communicate among internal and external stakeholders about cybersecurity risk

The NIST CSF is divided into five "Function" areas and each Function is divided into separate categories and sub-categories. A comprehensive Cybersecurity Program could adapt the NIST CSF and develop Cybersecurity Policies & Procedures to ensure all applicable Functions and Categories are adequately protected in the organization.



Source https://www.givainc.com/images/NIST-Cyber-Framework.png

ISO 21434

ISO / SAE 21434: Road Vehicles -- Cybersecurity engineering is, at the time of writing this document, being jointly developed by the International Organization of Standardization (ISO) and the Society for Automotive Engineers (SAE). The aim of this standard is to develop common terminology and criteria around key aspects of cybersecurity for the Automotive Sector. By applying the controls available in the standard, companies will be able to demonstrate due care and due diligence related to cyber-threat prevention in vehicle development, operations, maintenance and disposal.

> ***"In a connected world, the cybersecurity is as fundamental to your safety as the brakes."***
>
> *-Sir Ralf D Speth, the CEO of Jaguar Land Rover*

Applicable to **road-vehicles and their component systems**

Based on **current State-of-the-Art** for cybersecurity engineering

Goal of **reasonably secure** vehicles and systems

Risk-oriented approach

Automaters and suppliers can use to show **"Due Diligence"**

Management Activities for Cybersecurity

Focus on **Automotive Cybersecurity Engineering**

Cybersecurity activities/processess for **all phases of vehicle lifecycle**

Icons by Freepik on Flaticon.com

An important aspect of the ISO / SAE 21434 Standard is the emphasis placed on Threat and Risk Assessment (TARA). The results of this assessment controls the activities in the product development stage of the vehicle and enable the adoption of Cybersecurity Controls to safeguard the vehicle during its lifecycle. Although the standard emphasizes the need for a TARA, it does not describe a specific methodology for carrying out the TARA.

The standard also describes the overall in-vehicle cybersecurity architecture and mandates several processes that must be in place in the organization as well as in the supply chain. This means that any organization must develop an Information Security Management System (ISMS) in order to be in compliance with the standard. Specific controls such as policies, procedures and technical controls must be designed to implement such an ISMS. However, the standard itself does not propose any specific technologies.

Resources

Below are additional resources for Cyber Governance Frameworks for the Automotive Industry.

NIST Cybersecurity Framework	https://www.nist.gov/cyberframe-work
ISO 21434: Road Vehicles: Cybersecurity Engineering	https://www.iso.org/stan-dard/70918.html
Keys to Creating a Cybersecurity Process from the J3061 Process Framework	https://www.sae.org/learn/con-tent/c1730/
Free e-book on ISO 21434 Road Vehicles Cybersecurity Engineering.	http://iso21434guide.com/

6.0 - Cybersecurity Insurance

Despite an organization's best efforts to invest in IT security and governance, it is unfortunately impossible to completely eliminate all cyber risk. As a best-case scenario, a cyber incident will highlight a previously unknown or new vulnerability in an organization's IT infrastructure and allow for corrective action to avoid future occurrences. In the worst-case scenario, a cyber incident will shut down all operations, allow stolen data to fall into dangerous hands, and inflict financial losses on both the organization and its clients.

It's not just about privacy anymore...

Any business that uses digital technologies in its day-to-day operations carries a cyber risk, including those that do not collect personal information, such as B2B-focused companies. Whether it is the risk that an employee executes a programming error while maintaining a PLC, authorizes a wire transfer following the instructions presented in a social engineering scam, or clicks on a malware-infested file sent via a compromised business email (BEC), any organization is at risk for losses caused by a cyber breach.

Consider international shipping conglomerate Maersk who was the victim of the alleged state-sponsored NotPetya attack in 2017. The specific goal of the NotPetya virus was to destroy systems, not to steal private information or extort money. The unintended recipient of the virus saw its worldwide operations brought to a halt and were forced to revert to manual ways of conducting business and build what could be considered an entirely new IT infrastructure following the incident.

In terms of end-user devices, 49,000 laptops and all print capability were destroyed, and file shares were unavailable. All of Maersk's 1,200 applications were inaccessible — 1,000 of which were destroyed — while about 3,500 out of 6,200 servers were damaged beyond repair. Lost revenue from the attack was estimated to be in excess of USD $350 million.[1]

While this example is one of the largest publicly reported to date and commensurate with Maersk's size and operations, cyber breaches are not a matter of "if" but "when". Crippling cyber attacks are reported daily with no discrimination regarding the size of the organization, industry segment or geographical location. Every organization should ask themselves an important question: are we able to identify and quantify the financial impact arising from a cyber incident?

Insurance companies and brokers can help companies model the impact of a cyber incident and assist in optimizing risk strategies. One of those risk management solutions could involve transferring a portion of cyber risk to an insurance carrier.

... it's not one size fits all

There are two fundamental coverages provided by a typical cyber insurance policy.

The first covers the organization's own costs (first-party costs) in investigating and mitigating the effects of an actual or suspected cyber breach. These services are often offered via a list of pre-approved vendors and would include legal advice from a breach coach, a forensic investigation, notification to affected third parties and public relations consulting. Covered first-party costs also include indemnification for loss of income and additional operating expenses when business operations are interrupted or suspended due to a failure of network security (i.e. a denial of service attack). Modern-day cyber policies can also address exposures from cyber-attacks and business downtime caused by a breach at a key IT vendor site or cloud computing partner, and system failure stemming from non-malicious human operator errors.

First-party costs covered under a cyber insurance policy will also include more traditional expenses related to privacy breaches and the efforts necessary to contain and mitigate the impact of the incident. Breaches can arise from events such as the inadvertent transmission of viruses to third parties, the inability of an organization to prevent unauthorized access to confidential third-party information, or its participation in a Denial-Of-Service attack. First-party costs will reimburse an organization for the costs related to the set up of a call center, offering credit monitoring to individuals whose personal information may have been accessed, and responding to PCI-DSS or privacy investigations.

The second coverage offered by a cyber policy is third-party liability protection in the event of a privacy breach, which would include defence costs, amounts to settle or satisfy a judgment awarded to a third party, or payment of insurable fines levied by a privacy regulator. This coverage would apply whether the compromised personal information was that of a customer, vendor, or employee.

Additional coverages available through cyber insurance policies include:

- Cyber extortion: Coverage for first-party costs to deal with a cyber extortion threat, such as hiring a cyber extortion expert, as well as the amount of any ransom that is ultimately paid.

- Digital asset restoration: The cost to restore digital assets that are altered, damaged or destroyed due to a security breach.

- Reputational Harm: Loss of income directly resulting from adverse media about the insured's actual or alleged security, privacy, or media event that negatively and materially harms their reputation.

Cyber coverage gaps in other insurance policies

Property insurance

A property insurance policy is triggered by a physical peril such as a fire or flood and provides coverage for an insured's first-party losses arising from damage as a result of that peril. As such, while this policy might respond to cover the repair or replacement of computer hardware that is damaged or destroyed by a physical peril, it is not designed to cover the first-party or third-party losses that can arise from a cyber breach. In fact, many property policies contain a data or cyber exclusion that precludes coverage altogether for cyber or privacy breach losses. Some insurers offer an endorsement to property policies that provides partial first party cyber coverage to address some losses associated with the Internet of Things cyber risk exposure (i.e. physical damage as a result of a cyber breach). These endorsements typically do not cover ransom payments or forensics costs related to cyber extortion, and there has recently been widespread movement among insurers to reduce the available limits of this coverage.

Directors' and officers' liability insurance

Directors' and officers' (D&O) liability insurance provides coverage for corporations and their executives when they are faced with third-party management liability claims. While there are some potential third-party areas of coverage that could overlap between a D&O and a cyber insurance policy, cyber risk is primarily an entity exposure and the D&O policy is designed first and foremost to protect individual insureds. Coverage in a D&O policy is broadest for individuals, followed by private or not-for-profit (NFP) corporations, whereas public companies generally only have protection under D&O insurance for securities claims. One major area where a cyber policy provides coverage that is not available under a D&O policy is with respect to first-party costs that a corporate entity incurs when it experiences a cyber breach.

"A cyber incident is a problem for every automaker in the world, It is a matter of public safety."

(General Motors CEO Mary Barra)

Cyber coverage gaps in other insurance policies (continued)

Commercial crime insurance

A commercial crime insurance policy provides first-party coverage for loss arising from theft, burglary, fraud, and other dishonest acts carried out by the insured's employees or third parties with respect to the insured's "property" (as defined). A crime policy does not provide adequate coverage for cyber risk exposure because it covers the loss of tangible property and, as with a property policy, a problem arises under the crime policy when the loss involves intangible property such as data, namely there is no coverage. Further, crime policies require the insured to suffer a direct loss before coverage is available, and the theft of third-party personal or confidential information is not a direct loss to the insured. A typical crime policy (without amended language) will not cover first-party costs incurred as a result of a cyber or privacy breach (with the possible exception of data restoration costs) and will not respond to cover any associated liability to third parties.

Commercial general liability insurance

A commercial general liability (CGL) policy is triggered by third-party liability claims alleging bodily injury or property damage that arise out of the insured's premises, operations, products or completed operations. The policy can also cover an insured's advertising and personal injury liability. Although CGL policies do contain a broad scope of liability coverage, many CGL insurers have generally indicated that they do not intend to cover cyber risks and as such, CGL policies are even more likely than property policies to contain a cyber or data exclusion. Recent court decisions have also shown that insurers are willing to go to battle to prevent CGL policies from responding to cyber claims. In many cases insurers have been successful in arguing that cyber risks are not covered under CGL policies based on policy language as well as the fact that it was never their intent to provide that coverage. In instances where a court has found that cyber coverage is available under a CGL policy, insurers have been quick to amend the language to preclude a cyber claim from being covered again in the future.

"If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked"

(Richard Clarke – American Government Official)

The future of cyber insurance

Cyber insurance remains an emerging line of coverage but one that is rapidly expanding based on insurers' interest and capacity to follow the rapid evolution of cybercrime, and the types of threats and attacks preferred by perpetrators. Insurance companies continue to broaden coverage to include emerging trends such as cloud computing, bricking, voluntary shutdown of networks, cyber-terrorism, and more. To effectively protect your organization from the financial impact of a cyber incident, it is highly recommended that you consult with your risk manager or insurance advisor to determine the optimal approach to mitigate this enterprise risk.

"In 2018 we witnessed that a proactive approach to cyber preparation and planning paid off for the companies that invested in it, and in 2019, we anticipate the need for advanced planning will only further accelerate," said J. Hogg, CEO of Cyber Solutions at Aon. "Leaders must work to better insulate their companies and their processes, while simultaneously identifying the ways they can benefit from the opportunities offered through technology and digital transformation."

Additional Resources

Below are additional resources for enabling a Cybersecurity Insurance in the Automotive Industry.

Aon's 2019 Cybersecurity Risk Report, What's Now and What's Next.	https://cyber.aonunited.com/aon-top-cyber-risks-security-technology-data-digital-transformation?utm_source=mediare-lease&utm_campaign=cyber2019

Sources:

"NotPetya offers industry wide lessons", Computer Weekly, https://www.computerweekly.com/news/252464773/NotPetya-offers-industry-wide-lessons-says-Maersks-tech-chief

7.0 - Cyber Education & Awareness

As Connected & Autonomous Vehicles (CAV) become more prevalent, the Automotive Sector needs a workforce that is aware of Cyber threats and the impact they can have on an organization. This is critical to cultivating a corporate Cyber Culture. An important aspect of that is for all levels of the organization to have proper training and certifications as per their job profile.

Cyber Governance Awareness for Executive Management

It is imperative that C-level executives understand the critical nature of Cyber Governance as it relates to smooth operations and business success of their organization. Senior executives should be aware of the maturity level of Cyber Governance within their organization and ensure proper support and funding is available to the Cyber Governance team.

In addition, C-level executives must understand the current threats and the measures that must be taken to enhance the Cyber Profile of their organization. In this regard, the Siemen's Charter of Trust provides a holistic approach which Industry Leaders adopt:

"In the age of the internet of things, the cybersecurity is a crucial task. Our Charter of Trust initiative is a very important first step. We're open to many more partners. Cybersecurity is the key enabler for successful digital businesses as well as protecting critical infrastructure. We hope that this initiative will lead to a lively public awareness and, ultimately, to binding rules and standards."

- Joe Kaeser, CEO of Siemens

Image Source

Cybersecurity Awareness Training for ALL Employees of the Organization

It is imperative for an organization to ensure that all its employees undergo continuous Cybersecurity Awareness training. Such awareness-raising and security training plays a major role in changing the culture of Cybersecurity in an organization. Cybersecurity is everyone's responsibility and a continuous and ongoing Cybersecurity Awareness program ensures that everyone is aware of the risks that are faced by the organization. Some specific reasons to consider having all personnel undergo Cybersecurity Awareness Training are:

- Businesses have hundreds of thousands of client records stored in cloud infrastructure and databases that are often less defended as those of on-prem databases. These form lucrative targets for hackers looking to make a profit from selling such client records on the dark web

- Growing sophistication of cybersecurity attackers who have incorporated new technologies like Artificial Intelligence (AI) to automate their attacks means that only businesses that have heavily invested in cybersecurity have adequate protection

- Growth of mobile phone apps, big data, social media and web apps have increased the attack surfaces available to hackers to target businesses who utilize these technologies in their products

- OEMs often partner with Tier 1 & 2 Suppliers for their products and services. This means that hackers will often hack the Tier 1 & Tier 2 in order to gain access to the networks of the larger business (OEM)

- The increasing usage of cloud services to host startup data and processing mean that threats to cloud services have increased exponentially as well

Trainings / Certifications for Cybersecurity SMEs

The best way to ensure that your organization is protected from Cyber Threats is to build a workforce that has the knowledge and skillset to protect the organization. There are many Cybersecurity trainings and certifications focused on Cyber SMEs and these enable the organization to build a workforce that is resilient and futureproofs the organization from disruption and business losses. A comprehensive training program must be established in order to ascertain the needs for each role and relevant trainings provided to the personnel in those roles.

Resources

The below table details various industry certifications that are relevant for Cybersecurity SMEs.

Siemens Charter of Trust	https://press.siemens.com/global/en/pressrelease/char-ter-trust-takes-major-step-forward-advance-cybersecurity
Detailed online course on Automotive Cybersecurity concepts.	http://automotivecybersecuritycourse.com/
Offers Cyber Governance certifications such as CISA and CISM.	https://www.isaca.org/pages/default.aspx
Offers Cyber Governance certifications such as CISSP and CSSP.	https://www.isc2.org/
Cybersecurity Awareness	https://www.bestcybersecurityawareness.com/
Offers certifications such as CEH and CCISO.	https://www.eccouncil.org/
Best practice guide for security awareness & training	https://www.automotiveisac.com/best-practices/
APMA podcast on Cybersecurity	https://soundcloud.com/user-819903760/intelligent-pod-cast-cyber-security
APMA podcast 2 on Cybersecurity	https://soundcloud.com/user-819903760/cyber-securi-ty-part-2
Canada's Little Black Book of Scams	https://www.ic.gc.ca/eic/site/cb-bc.nsf/eng/04333.html

8.0 - Risk Mitigation Techniques

With the advent of Connected Vehicles / Autonomous Vehicles (CV/AV), the existential dimensions of Cyber Risk have become manifest to OEMs, Tier 1s and Tier 2s. The adoption of ISO 21434 means that OEMs need to address Cyber Risk both from an enterprise-wide perspective as well as from the Supplier perspective. This means delegating responsibility of this initiative to the CISO who can work with the CIO as well as the business units to formalize a Risk Management Strategy.

A true partnership between all these stakeholders is essential as no single leader or team can gain the complete perspective needed to be effective in the Cyber domain, especially in the Automotive sector. This is because, due to the large number of suppliers for any OEM, no one group within the company could manage the number and types of internal and external threats, the complex technological landscape, and the many actions needed to address vulnerabilities associated with people and technology.

Incident Response Planning

A critical component of Risk Management is an Incident Response Plan (IRP). The main objectives of an IRP are to detect, identify and respond to and recover from cybersecurity incidents. This means that the Incident Response Plan ultimately prevents damages like service outage, data loss or theft, and unauthorized access to organizational systems.

An incident response team (IRT) that owns the responsibility of developing, testing and carrying out the IRP needs to be created. The IRT are Cyber SMEs who have the training, expertise and the experience to collect, analyze and act upon information from an incident. The IRT is also responsible for "owning" the incident response and communicating with other stakeholders within the organization, and external parties such as legal counsel, media, law enforcement and affected customers.

Vulnerability Scanning / Penetration Testing

Today's Cyber-physical systems are often updated in an Over-The-Air (OTA) fashion; in particular, modern Connected Vehicles receive OTA updates. Vulnerability Management then becomes (especially in the context of OTA updates) an essential part of the Automotive organization's Cyber Governance Program. Vulnerability management includes assessing, mitigating and reporting on any security vulnerabilities that exist in an organization's systems and software, including software updates. Vulnerabilities in Vehicle systems can be exploited, potentially leading to hacks or other damaging attacks. Therefore, these vulnerabilities must be managed by discovering, identifying and patching them.

Vulnerability Scanning is the process by which systems are scanned for vulnerabilities and reports generated to mitigate them. Penetration Testing is a more intrusive exercise where the vulnerabilities found during the scanning phase are used to exploit and hack into the target systems.

Continuous Monitoring

Continuous monitoring is a vital step for Automotive organizations to identify and measure the security implications for planned and unexpected changes to hardware, software, firmware and to assess vulnerabilities in a dynamic threat space. Continuous monitoring is one part of a six-step process in the NIST Risk Management Framework (RMF), from NIST publication 800-53, rev4. NIST defines continuous monitoring as "a formalized process where an entity can define each of its systems, categorize them by risk level, apply the appropriate controls, and continuously monitor the controls in place and assess their effectiveness against threats in their environment."

CIA Info Security Triad

Resources

Below are additional resources for enabling Risk Mitigation Strategies.

CanCyber	CanCyber provides real time threat indicator sharing and tools to turn indicators into action. Powered by MISP, Yara, and Zeek Network Security Monitor (BroIDS), export indicators into your own equipment or use our malware hunting tools on the endpoint, domain, or network.	https://cancyber.org/
Automotive ISAC	Has best practice documentation on Incident Response, Threat Detection, Monitoring and Analysis	https://www.automotiveisac.com/best-practices/

9. Supply Chain Cyber Assessment

Due to the unique nature of the automotive industry, the automotive supply chain is long and complex. With the advent of the Connected and Autonomous Vehicle (CAV), this supply chain now includes tech vendors as well as Cloud Apps. Furthermore, OEMs and other automotive entities are reliant on third parties such as data centers andservice providers. A break in the chain at any one point (or even a minor vulnerability that cn be exploited, whether an OEM, a supplier or a Service Provider) can be disastrous for the end-consumer (i.e. the passengers in the vehicles).

Vendor Cyber Risk Assessment Program

The challenge for most organization is to effectively manage the Cyber risk from the diverse number of suppliers found in their supply chain. In order to meet this challenge, a comprehensive Vendor Cyber Risk Assessment Program needs to be developed. Such a program requires Cyber SMEs with a unique skillset that carry out continuous assessment of its suppliers. Such a program mitigates the potential for a damaging Cybersecurity breach attributed to the cyber practice failings of a vendor. A Vendor Cyber Risk Assessment Program also has several other benefits including more positive commercial relationships, decrease in risk exposure due to supplier service failures or non-compliance, and reduces the chances of the supplier not adhering to contractual obligations.

Cloud Apps Risk Assessment

Developing a Cloud Apps Risk Assessment Policy is an essential component of a modern Vendor Cyber Risk Assessment Program. Having such a policy in place ensures that the organization can regulate the use of applications and infrastructure resources that users access in the Cloud. Such a policy also helps to ensure that the organization's confidential information and data is protected and remains uncompromised.

The main objective of a Cloud Apps Risk Assessment Policy is to establish a standard of practice for the procurement, risk evaluation, and use of SaaS Apps that the organization relies on. By applying this policy, the organization can establish a level of Cyber guidance when procuring SaaS Apps, managing users, protecting data, and securing assets in the Cloud.

Resources

Below are additional resources for Cyber Governance Frameworks for the Automotive Industry.

Auto ISAC best practice guide for Collaboration & Engagement with 3rd Parties.	https://www.automotiveisac.com/best-practices/

Appendix 1

Transport Canada Principles of Automotive Cybersecurity

Transport Canada has focused on developing Principles of Automotive Cybersecurity. The aim is to provide clear and consistent guidance principles for the Production, Utilization, Maintenance and Disposal of Connected and Automotive Vehicles (CAV) in Canada.

More details can be found at https://www.tc.gc.ca/en/transport-canada.html

Canadian Centre for Cybersecurity

The Canadian Centre for Cybersecurity *https://cyber.gc.ca/en/* was launched on 1 October 2018 as part of the Communications Security Establishment (CSE), the Canadian Centre for Cybersecurity (Cyber Centre) is a new organization but one with a rich history. The Cyber Centre brings operational security experts from across the Government of Canada under one roof. In line with the National Cybersecurity Strategy, the launch of the Cyber Centre represents a shift to a more unified approach to Cybersecurity in Canada.

The Canadian Centre for Cybersecurity will:

- Be a clear, trusted source of relevant Cybersecurity information for Canadians, Canadian businesses and critical infrastructure owners and operators.

- Provide targeted Cybersecurity advice and guidance to protect the country's most important cyber systems.

- Develop and sharing our specialized cyber defence technology and knowledge, helping to improve Cybersecurity for all Canadians.

- Defend cyber systems, including Government of Canada networks, by developing and deploying sophisticated cyber defence tools and technology.

- Lea the Government's operational response during cyber events by using our expertise and access to provide information immediately useful for managing incidents.

- Cyber defence is a team sport. Our unique advantage helps make Canada more resistant to cyber threats and more resilient during and after cyber events.

The baseline Cybersecurity controls for small and medium organizations in Canada that want recommendations to improve their resiliency via Cybersecurity investments.

Other Global Automotive Cybersecurity Initiatives

The below table details various industry certifications that are relevant for Cybersecurity SMEs.

Voluntary Guidance

SAE Guide Book on J3061 standard	https://www.sae.org/standards/content/j3061_201601/
5 Stars Rating – UK (Horiba MIRA, Thatcham, Ricardo Roke and Axillium Research) – 2019	https://saemobilus.sae.org/cybersecurity/news/2019/04/5-stars-consortium-to-use-five-star-rating-system-for-automo-tive-cyber-security
Cybersecurity Act – EU (ENISA) EU Wide Certification Framework products, services and processes - 2019	https://ec.europa.eu/digital-single-market/en/eu-cybersecu-rity-act
Thatcham Insurance Guidelines – Cybersecurity Requirements 2019	https://www.thatcham.org/what-we-do/security/
Auto ISAC Best Practices	https://www.automotiveisac.com/best-practices/

Mandatory Regulations

UNECE Cybersecurity and SW Update Regulations – Release 2019, Effective 22CY (EU & Japan)	https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp-29grva/GRVA-01-18.pdf
NHTSA V2V NPRM	https://www.nhtsa.gov/technology-innovation/vehicle-vehi-cle-communication
NHTSA AV ANPRM	https://www.nhtsa.gov/vehicle-manufacturers/automat-ed-driving-systems

Acknowledgments

Flavio Volpe
President, APMA

APMA
LEAD. REACH. CONNECT.

The Automotive Parts Manufacturers' Association (APMA) would like to express their great appreciation to its CTO, **Colin Dhillon** for taking the initiative and creating the APMA Cybersecurity Committee. Your continued leadership in the growing technology sectors, for both our members and our association is very much appreciated. To **Mr. AJ Khan**, President and CEO of Cloud GRC, and Co-Chair of the APMA Cybersecurity Committee, for his efforts in both planning and development of the CyberKit 1.0. To **Ms. Catherine Bertheau**, Cyber Solutions Business development Lead (Eastern Canada) of Aon, and **Mr. Philip Lafrance**, Standards Manager at ISARA for their diligent review work on the CyberKit 1.0. Your willingness to give your time so generously has been very much appreciated.

Colin Dhillon
Chief Technical Officer,
apmaTEC

AJ Khan
President & CEO.
Cloud GRC

Catherine Bertheau
Cyber Solutions Business
development Lead,
Aon

Philip Lafrance
Standards Manager,
ISARA

The APMA would also like to thank the members of the cybersecurity committee for their continued support and efforts in helping to identify the initiatives surrounding the ideation, development and creation of the APMA's CyberKit 1.0. Your generously has been very much appreciated.

Adam Mallory, VP Blackberry QNX
Todd Bielarczyk, Intelligence Officer CSIS
José Fernandez, Cybersecurity Element AI
John Wright, Founder & Chairman JPOM
John Heaton Partner, Cybersecurity KPMG
Ganesh Iyer, CIO & VP of Eng. Martinrea
Charles Finlay, Executive Director Rogers Cybersecure Catalyst (Ryerson University)
Oliver Winkler, Business Leader, Strategy & Innovation Siemens
Romeo Ware, CEO Three Lefts
Dr. Mitra Mirhassani, Associate Professor University of Windsor
Hassan Al Bouhali, SVP IT and Digital Transformation Woodbridge Group

Contact us

apmaTEC
Division of APMA

Colin Singh Dhillon
Chief Technical Officer
T: 416.620.4220 ex.232
C: 416.428.5288

Automotive Parts Manufacturers' Association. 10 Four Seasons Place, Suite 801 | Toronto, Ontario. M9B 6H7 | Canada


SEIBU
SEIBU
miu miu
ZARA