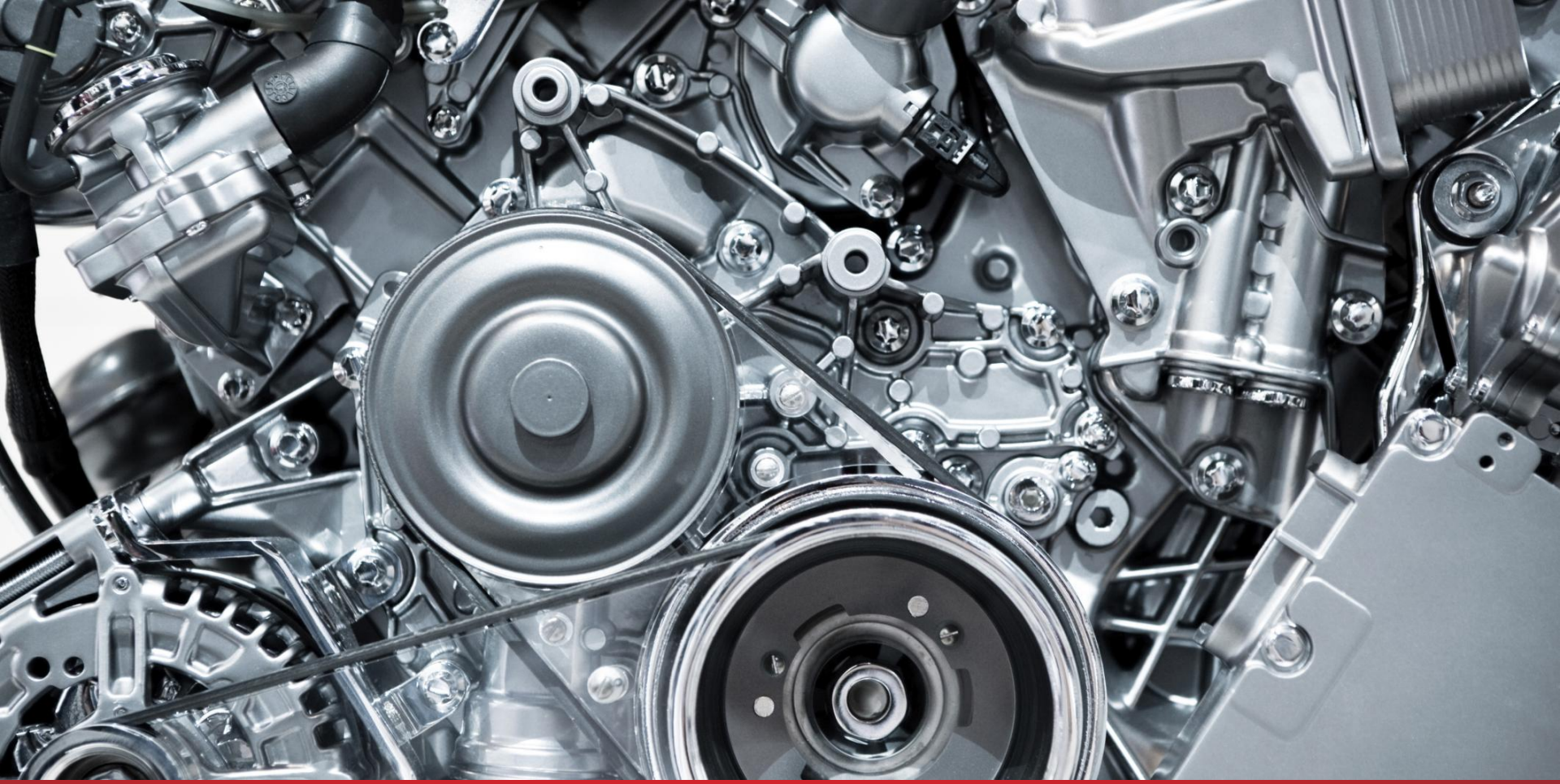


OESA West Coast Regional Supplier Meeting

Hacking and Tracking:
Cybersecurity, Privacy & Data Ownership

BUTZEL LONG

Claudia Rast

Outline

- Automotive **Cybersecurity**
  - Is it any different than the concerns in other industries?
- **Privacy** in the Automotive Context
  - Special consideration re V2X
- The **Data Ownership** Free-for-All
  - So many "authors" so many owners
- **Best Practices** re Cybersecurity

Hacking & Tracking

AUTOMOTIVE CYBERSECURITY

BUTZEL LONG
AUTOMOTIVE INDUSTRY PRACTICE

Automotive Cybersecurity

- The Unique Aspects of Automotive Cybersecurity
  - Identifying the Risks
  - Protecting by Design (Security & Privacy)
  - Implementing Defenses
  - Responding to Infiltrations / Exfiltrations
  - Recovering Post-Incident

NHTSA & Cybersecurity

- 2012: NHTSA modified its research organization to focus on vehicle electronics, including cybersecurity, establishing a new division, **Electronic Systems Safety Research**, to conduct research on the safety, security, and reliability of complex, interconnected, electronic vehicle systems.
- More recently, NHTSA expanded its research and testing capabilities in vehicle electronics at the **Vehicle Research and Test Center in East Liberty, Ohio**.
- These two newly organized entities execute research programs in three main areas:
  - electronics reliability (including functional safety)
  - automotive cybersecurity
  - automated vehicles
- These entities are responsible for evaluating, testing, and monitoring potential automotive cyber vulnerabilities, and for leading the agency's research of highly automated vehicles.
- NHTSA also established an internal agency working group, the **Electronics Council**
  - responsible for collaborating on issues related to vehicle electronics, including cybersecurity, across the entire NTHSA organization with particular focus on the Research, Rulemaking, Data, Enforcement, and Chief Counsel offices

Cybersecurity Risks

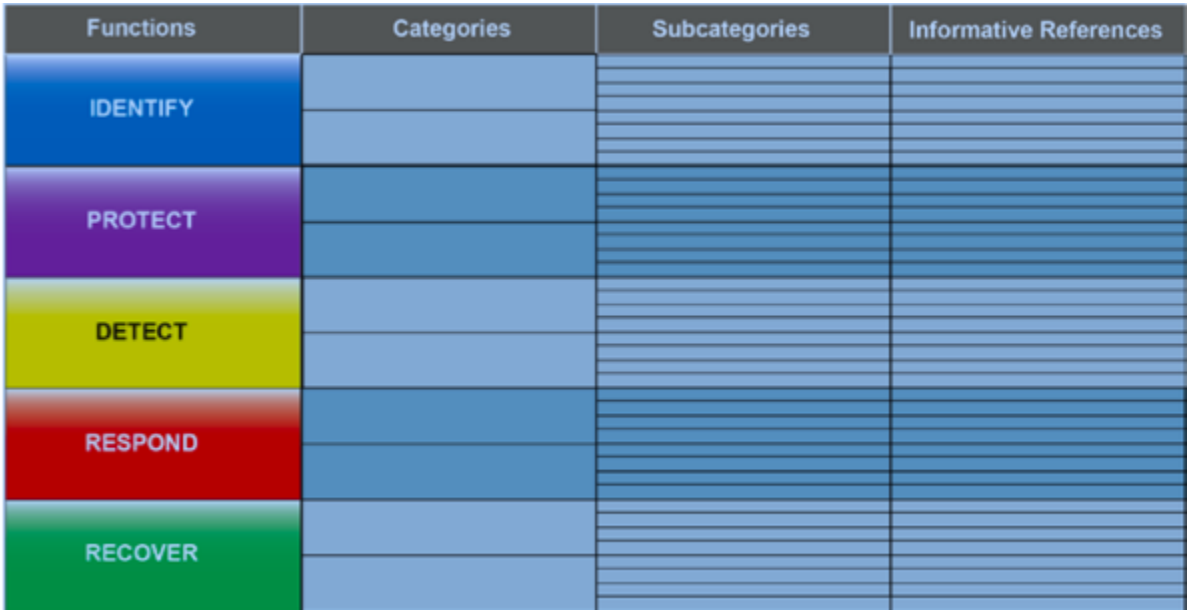
- Hacking as a Service
- Ransomware (data encryption-extortion)
- Smartphone Kidnapping
- GPS Data Theft
- Social Engineering
- Infotainment malware
- Hackers abusing Cloud Services
- V2V Spoofing
- Automotive Spear Phishing
  - Fraudulent Speeding Tickets

BUTZEL LONG
AUTOMOTIVE INDUSTRY PRACTICE

Current Federal Standard: NIST

NIST Cybersecurity Framework:

- Identify
- Protect
- Detect
- Respond
- Recover



BUTZEL LONG
AUTOMOTIVE INDUSTRY PRACTICE

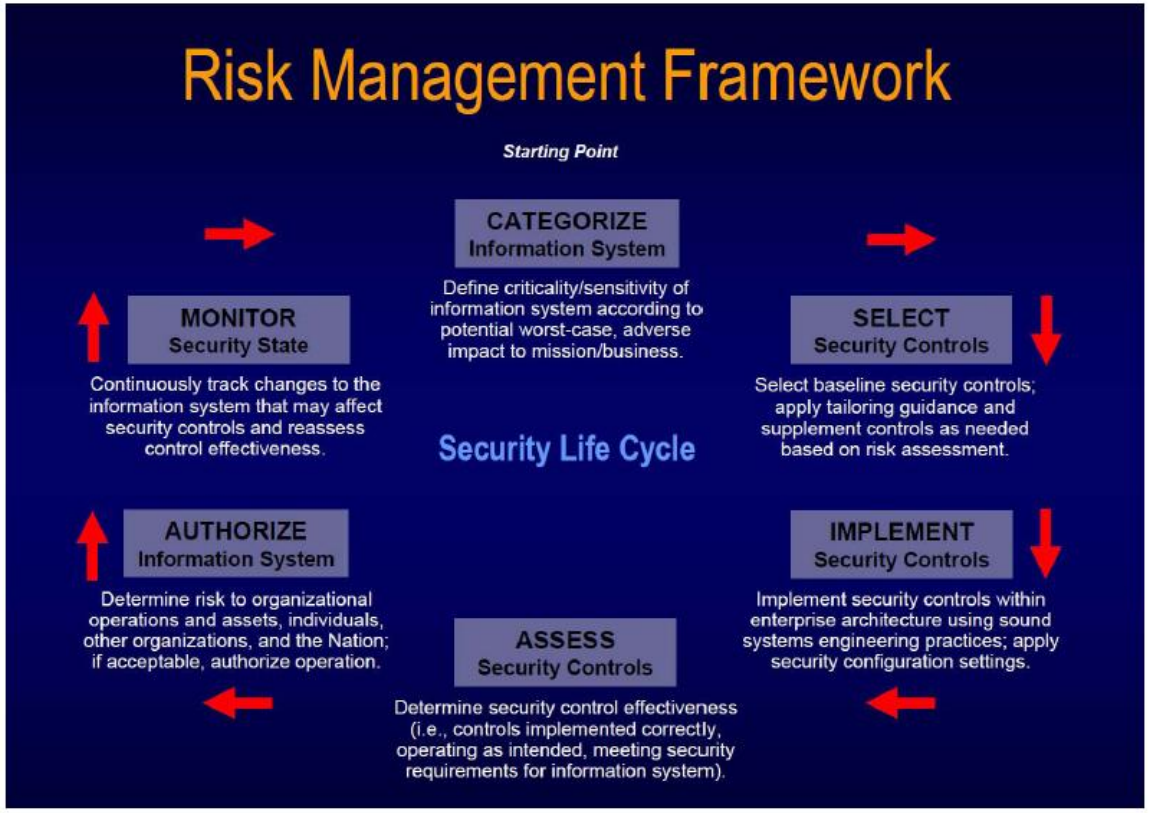


Figure 1: NIST Risk Management Framework (RMF)

BUTZEL LONG

NIST Risk Management Framework

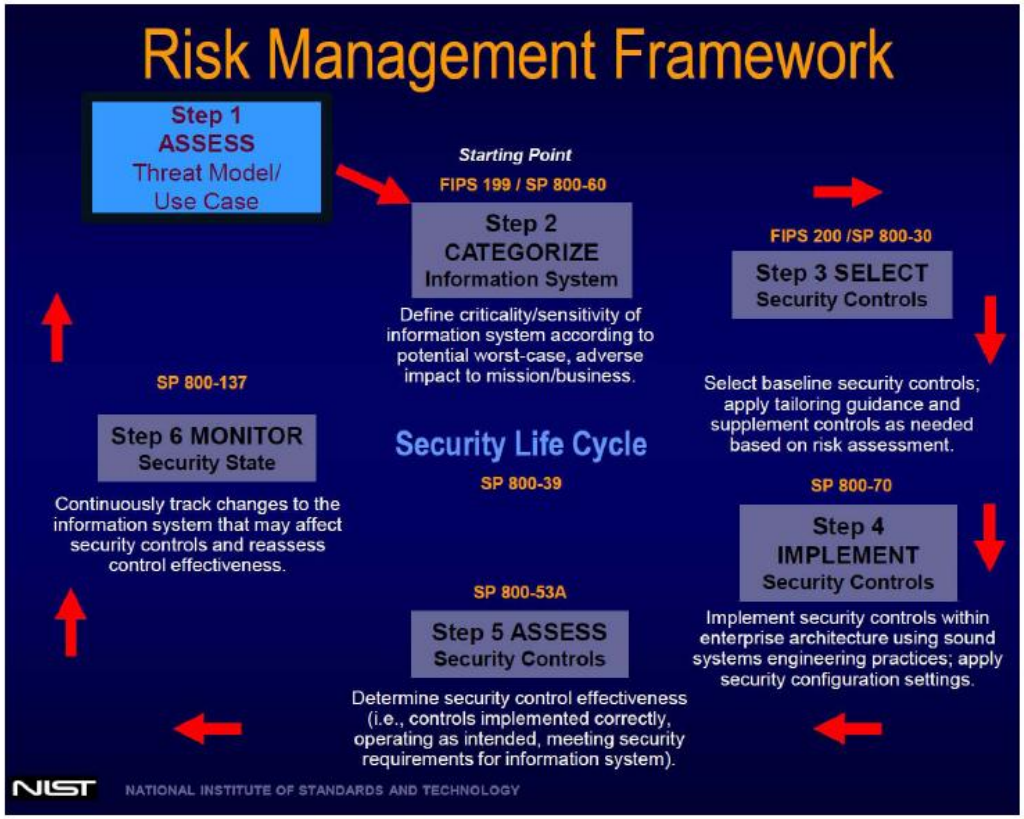


Figure 2: Modified NIST Risk Management Framework for the Vehicle Sector

Apply the Risk Management Framework to the Vehicle Sector

BUTZEL LONG

Hacking & Tracking

DATA PRIVACY

BUTZEL LONG
AUTOMOTIVE INDUSTRY PRACTICE

The Two-Sided Coin: "Data Privacy" and "Data Security"

Understanding the overall privacy and security landscape helps to set the tone for the protections we must provide

- ***Data Privacy***: the relationship between the collection, storage, use, dissemination and security of information identifiable or defined as private, the varying public expectations (or not) of privacy, and the attendant legal and political tensions

- ***Data Security***: the protection of data from any unauthorized access in violation of policy, law, regulation or rule

BUTZEL LONG
AUTOMOTIVE INDUSTRY PRACTICE

Living with Current and New Laws: Data Privacy

Apply principals of privacy by design:

- Be proactive, not reactive; be preventative and not remedial
- Privacy is the default setting
- Privacy is embedded into the design and architecture
- Full functionality, positive-sum and not zero-sum
- End to end security – full lifecycle protection
- Visibility and transparency
- Respect for user privacy – keep the architecture user-centric

Consumer Privacy Protection Principles – Nov 2014

Alliance of Automobile Manufacturers & **Association of Global Automakers**

- Published "**Consumer Privacy Protection Principles**," sent→FTC
- Offers baseline privacy commitments for automakers
- based on the Fair Information Practice Principles, which have served as the basis for privacy frameworks in the US and around the world for over 40 years

Seven Principles:

- **Transparency** among automakers re collected / shared information
- **Choice** re data collected
- **Respect for Context**
  - impact of collected data on drivers
- **Data Minimization, De**
- **-Identification & Retention**
- **Data Security**
- **Integrity & Access**
- **Accountability**

V2V Privacy Overview

- ✓ V2V system is designed to address multiple technical, physical & organizational controls to minimize privacy risks, including the likelihood of vehicle tracking by individuals and government or commercial entities

- PKI security →enable trust without requiring PII
- Safety Messages **will not contain PII** that identifies the car, its driver or owner; no PII for enrollment or safety recall purposes
- V2V devices **will transmit** safety messages in only a **limited** geographical range
- V2V system will **not collect** or store **safety messages except** in the limited case of device malfunction
- Separation of functions/data within the SCMS *(Security Credential Management System)*

V2V NPRM Privacy Impact Assessment (PIA)

- **What is a PIA?**
  - Documents the flow of personal information/information requirements within a system -- how and why information is transmitted, collected, stored and shared
  - Assesses the potential risks and effects on individual privacy of the proposed data transactions
  - Examines and evaluates protections (called "controls") and alternative processes for handling data to mitigate potential privacy risks
  - Identifies risk that cannot be mitigated (called "residual risk")
- **Why Conduct a PIA?**
  - Required by eGovernment
  - Provides public with documented assurance that NHTSA has identified and appropriately addressed potential privacy issues resulting from V2V NPRM
  - Facilitates informed regulatory policy decisions by enhancing an agency's understanding of privacy risk, of options available for mitigating that risk, and of residual risk that cannot be mitigated (and whether some functionality should be sacrificed to mitigate risk further)

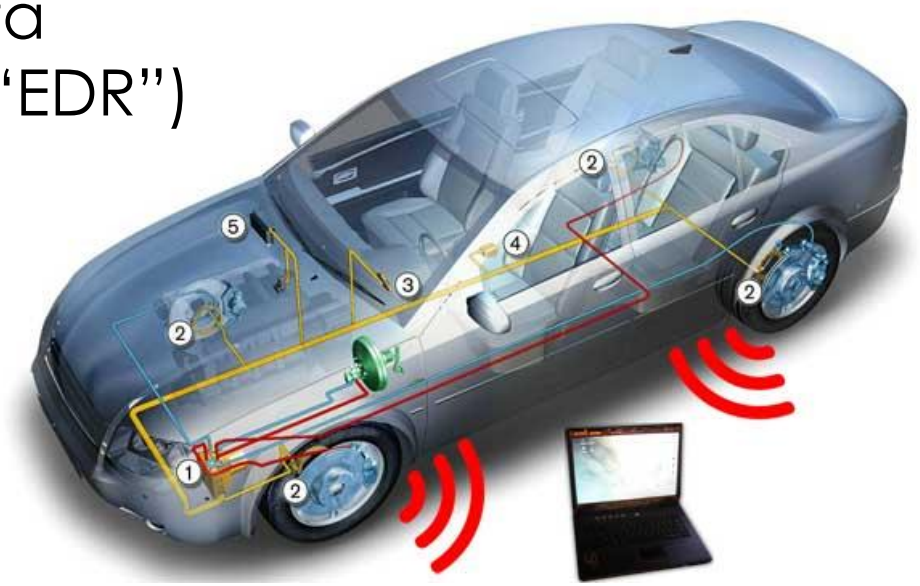
Hacking & Tracking

DATA OWNERSHIP

BUTZEL LONG
AUTOMOTIVE INDUSTRY PRACTICE

Addressing Data Concerns

- What types of data exist?
  - Geo-location
  - Vehicle behavioral data
  - Event Data Recorder ("EDR")
- How is it generated?
  - Automatically (EDR)
  - Opt In (Apple Play)
- Where is it kept?
  - Locally (the vehicle)
  - The "Cloud"
  - Data Centers (foreign and domestic)



BUTZEL LONG
AUTOMOTIVE INDUSTRY PRACTICE

What is a Copyright?

- A grant to the author of the exclusive right to duplicate, transcribe and imitate his/her original "work" of authorship and derivative versions
- Traditional examples: Books, Music & Lyrics, Movies, TV Shows, Periodicals
- Common today: Website Design & Content, Social Media Content

 Claudia Rast
Rast@butzel.com

What Cannot Be Copyrighted?

- **Titles, names, short phrases**, and slogans; familiar symbols or designs; mere variations of typographic ornamentation, lettering, or coloring; mere listings of ingredients or contents (much of this can be trademarked)
- **Ideas**, procedures, methods, systems, processes, formulas, concepts, principles, discoveries, or devices, as distinguished from a description, explanation, or illustration of them
- Works consisting ***entirely*** of **information that is common property** and containing no original authorship (for example: standard calendars, height and weight charts, tape measures and rulers, and lists or tables taken from public documents or other common sources)
- ***Works produced by a machine or by a mere mechanical process which operates randomly or automatically without any creative input or intervention from a human author***

Claudia Rast
Rast@butzel.com

BUTZEL LONG
AUTOMOTIVE INDUSTRY PRACTICE

Who (or What) is the Author?

- The **author** of an **original work** has the **exclusive right of ownership**
- Five potential authors:
  - the **programmer** of the device,
  - the **user** or wearer of the "thing",
  - **both** the programmer and the user,
  - the **device**, or
  - **no one**.

 Claudia Rast
Rast@butzel.com

Humans Rule (for now)

- The US Copyright Office will only register a Work if it was created by a human being
- IP law protects **the fruits of intellectual labor** that are **founded in the creative powers of the mind**

 Claudia Rast
Rast@butzel.com

So, Who Owns the Data?

- Who ***wants to own*** the data?
  - Vehicle owner
  - OEM / Tier 1 / Tier 2
  - Third Parties: insurance companies, etc.
- Who ***actually*** owns the data?
  - Check State Law: vehicle owner or lease holder (codified in Arkansas, California, Colorado, Connecticut, Delaware, Maine, New Hampshire, New York, Nevada, North Dakota, Oregon, Texas, Utah, Virginia and Washington)
  - Look at the Contract

 Claudia Rast
Rast@butzel.com

BUTZEL LONG
AUTOMOTIVE INDUSTRY PRACTICE

Ownership Requires Careful Analysis

- What Data Points are at Issue?
- Who or What Created the Data?
- Is the Data an Original Work of Authorship? (i.e., was a Human involved?)
- Is there a Contract specific to the Data?
- Is there a relevant State Statute?

 Claudia Rast
Rast@butzel.com

BUTZEL LONG
AUTOMOTIVE INDUSTRY PRACTICE

Finally

If the Data is important to you, negotiate the IP rights up front!

 Claudia Rast
Rast@butzel.com

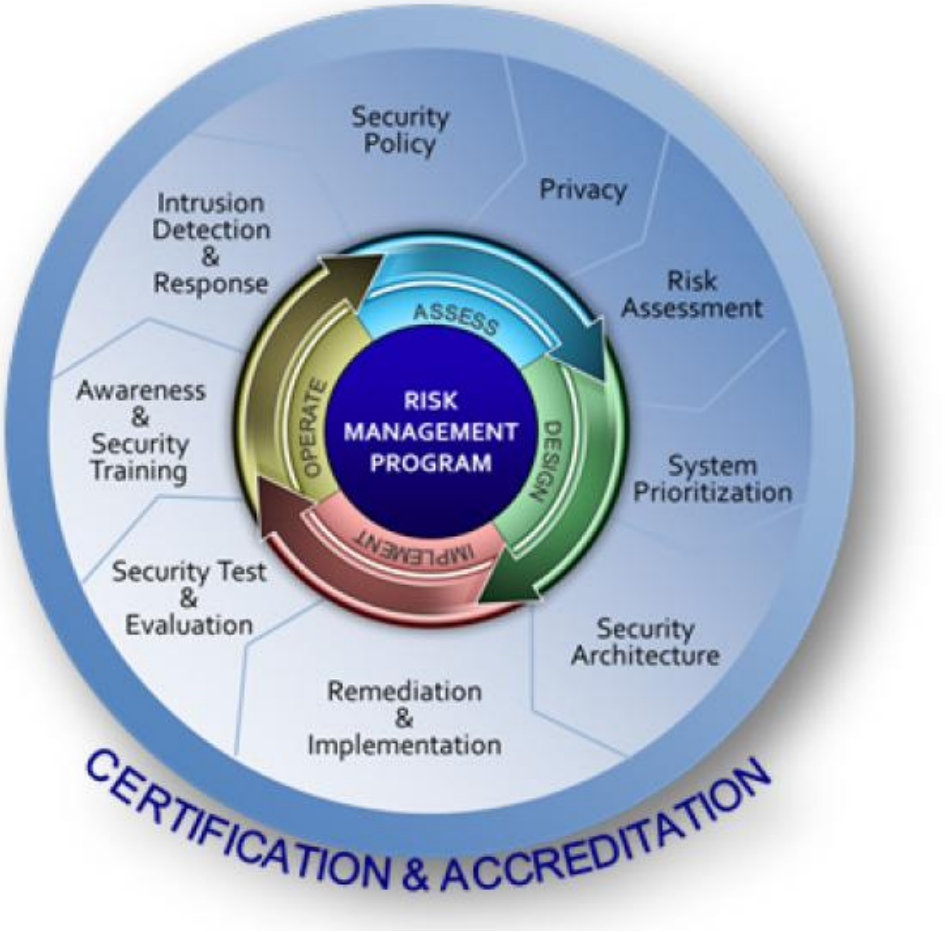
BUTZEL LONG
AUTOMOTIVE INDUSTRY PRACTICE

Hacking & Tracking

BEST PRACTICES

BUTZEL LONG
AUTOMOTIVE INDUSTRY PRACTICE

Information Security Life Cycle



Mapping Auto Cyber Best Practices

Best Practice Examples Identified	Assess					Design		Implement	Operate
	Establishing a Security Policy	System Security Evaluation	Iterative Risk Assessment	System Prioritization	Security Architecture	Remediation and Implementation	Security Test and Evaluation	Awareness and Security Training	Intrusion Detection and Response
Aviation As Parallel Industry	✓	✓	✓	✓	✓	✓	✓	✓	✓
Strong Federal Leadership	✓	✓	✓	✓	✓	✓	✓	✓	✓
End-to-End Connected Vehicle Security	✓	✓	✓	✓	✓	✓	✓	✓	✓
Leveraging International Cybersecurity Efforts	✓			✓	✓			✓	
Fostering Industry Cybersecurity Groups	✓				✓	✓		✓	✓
Ongoing Shared Learnings With Other Federal Agencies	✓	✓			✓	✓		✓	✓
Cybersecurity Is A Lifecycle Process	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cybersecurity Standards For Entire Supply Chain	✓				✓	✓	✓		
System Design And Operators Cyber Acumen	✓	✓	✓	✓	✓	✓	✓	✓	
Identify Minimum Security Requirements	✓	✓	✓	✓	✓	✓	✓	✓	✓
Develop A Cybersecurity Simulator		✓	✓	✓	✓	✓	✓	✓	✓
Identify A Standards Development Baseline	✓	✓	✓	✓	✓	✓	✓	✓	

BUTZEL LONG
AUTOMOTIVE INDUSTRY PRACTICE

Best Practices for Management

- Perform Risk Assessment (Physical Plant, Information Systems & Workforce)
- Segregate & Secure High Risk Information, Operations & Workers
- Encrypt Sensitive Data/Implement Robust Password Policy
- Implement Company-wide Training (Ongoing)
- Incorporate Security By Design (i.e., from the beginning)

Best Practices for Management

- Acquire Cyber Liability Insurance
- Enable Network Security Monitoring & Review of Log Files (Lesson Learned from Target)
- Demand Compliance from Contractors & Suppliers (Another Lesson from Target)
- Conduct Table-Top Drills
- Have Experts at the Ready If/When an Attack Occurs

Best Practices for IT Departments

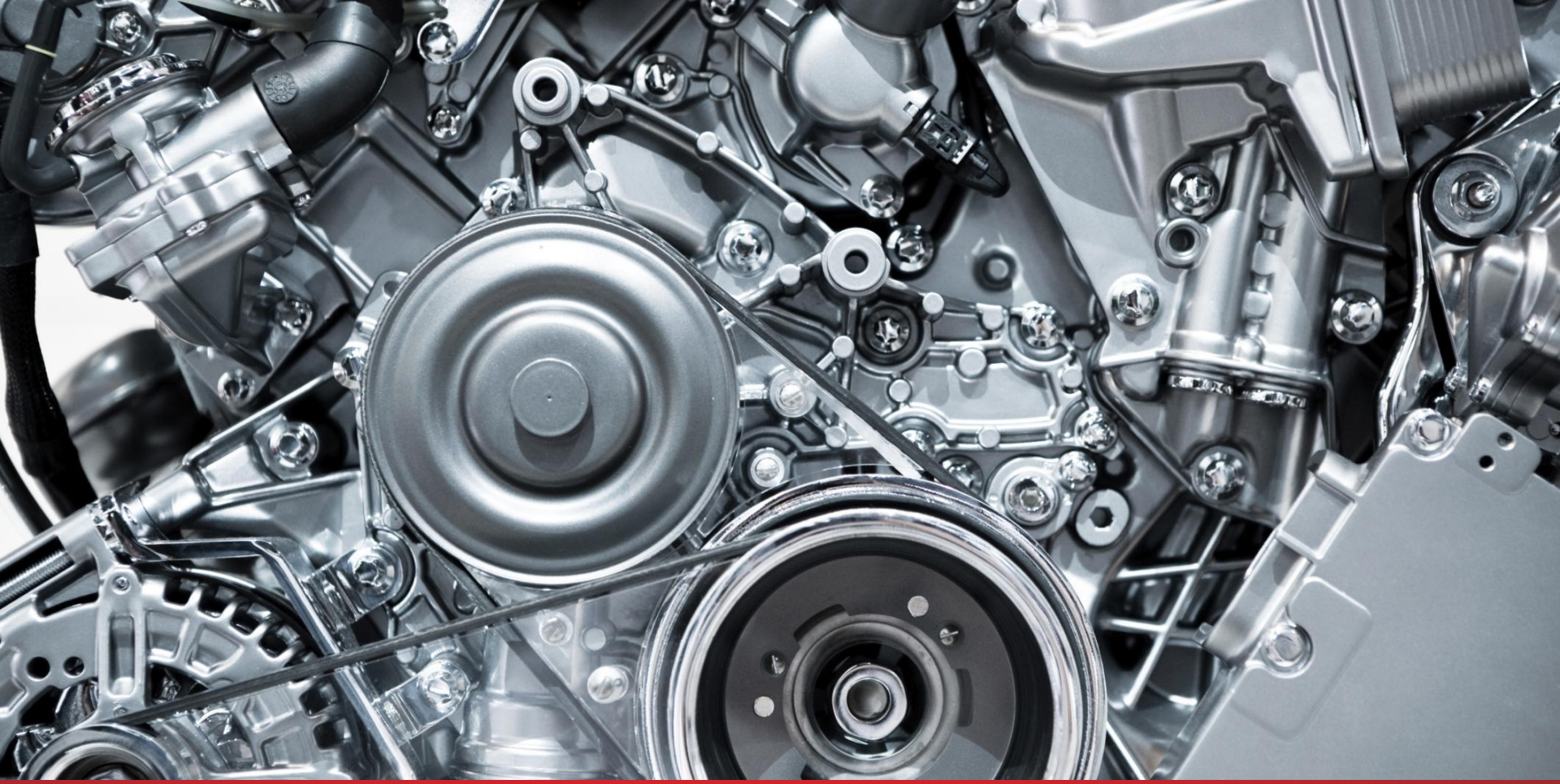
- Eliminate Unnecessary Data
- Conduct Ongoing & Active Risk Analysis
  - Vulnerability testing (external & internal)
- Collect, Analyze & Share Incident Data
- Collect, Analyze & Share Tactical Threat Intelligence, Especially Indicators of Compromise
- Focus on Better & Faster Detection
  - Log files & monitoring post CISA

Best Practices for IT Departments

- Use Metrics to Drive Security – Unusual Activity?
- Evaluate Threat Landscape to Prioritize Treatment Strategy
- Track Workforce: Who's Who, What they Do & When they Go
- TEST Backups
- Encrypt
- Patch, upgrade & update

For More Information: Technology Resources

- National Institute of Standards and Technology ("NIST").
  - NIST Framework for Improving Critical Infrastructure Cybersecurity
  - NIST Special Publication No. 1800-4b
  - NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems
  - NIST Special Publication 800-52: Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations
  - NIST Special Publication 800-77: Guide to IPs and VPNs
  - NIST Special Publication 800-88: Computer Security
  - NIST Special Publication 800-111: Guide to Storage Encryption Technologies for End User Devices
  - NIST Special Publication 800-113: Guide to SSL VPNs
- Federal Information Processing Standards: FIPS 140-2.
- NHTSA and Vehicle Cybersecurity:
  http://www.nhtsa.gov/About+NHTSA/Speeches,+Press+Events+&+Testimonies/NHTSA+and+Vehicle+Cybersecurity



Questions? Thank You!

BUTZEL LONG