Potter Anderson Corroon LLP

YOUR DELAWARE ADVANTAGE

Privacy and Cyber Risk in a Connected World

Secure Delaware Workshop

William R. Denny

October 4, 2022

Presenter: William R. Denny

- Partner and Chair of the Cybersecurity, Privacy and Data Governance Practice at Potter Anderson & Corroon LLP, Wilmington, Delaware
- Certified Information Privacy Professional (CIPP/US) and Certified Information Privacy Manager (CIPM) by the International Association of Privacy Professionals
- Member of the ABA Cyber Security Legal Task Force

Agenda

- What are Connected Technologies?
- What are the principal privacy and cyber concerns?
- What are the laws and regulations involved?
- Examples – Connected Cars & IoMT
- Managing Risk
- What Next?

Connected Technologies

"Connected Technologies" generally refer to products that have internal or built-in technology that allows it to communicate – or connect – with other products, devices, people, etc. in the external environment.

This universe of connection may be referred to as the Internet of Things (IoT)

Examples include smart phones, video conferencing, fitness wearables, home fixtures and appliances, telehealth, connected vehicles, drones, network routers, surveillance cameras, payment devices.

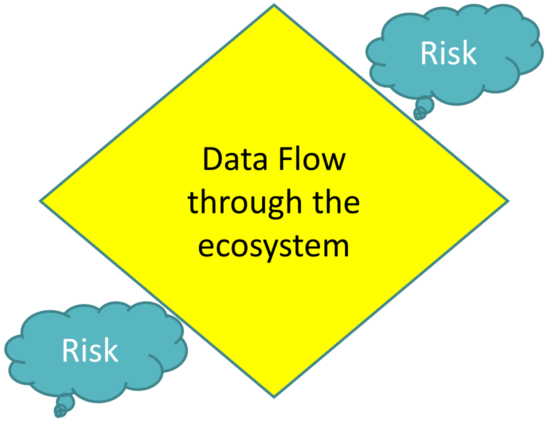
With increasing connections comes additional functionality, accessibility, ease and benefit. But not without risks….

Connections and Technologies

Technologies

Existing products with new technology – phones, fridge, watches, cars

New Products developed to be part of the ecosystem



Connections

- Cloud/ SaaS platforms
- Satellites
- 5G
- Blockchain
- Other new technologies

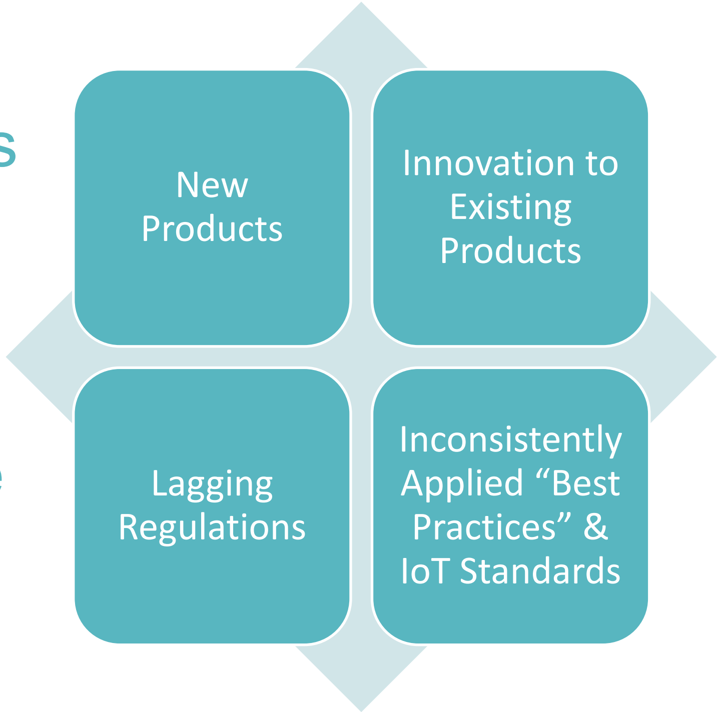
Applications

- New applications to facilitate connections and functionality
- Role of Third Parties

What’s the Big Deal?

✓Key privacy and security concerns are common across products and industries

✓Constant evolution in the regulatory landscape and the definition of “best practice.”



New Products

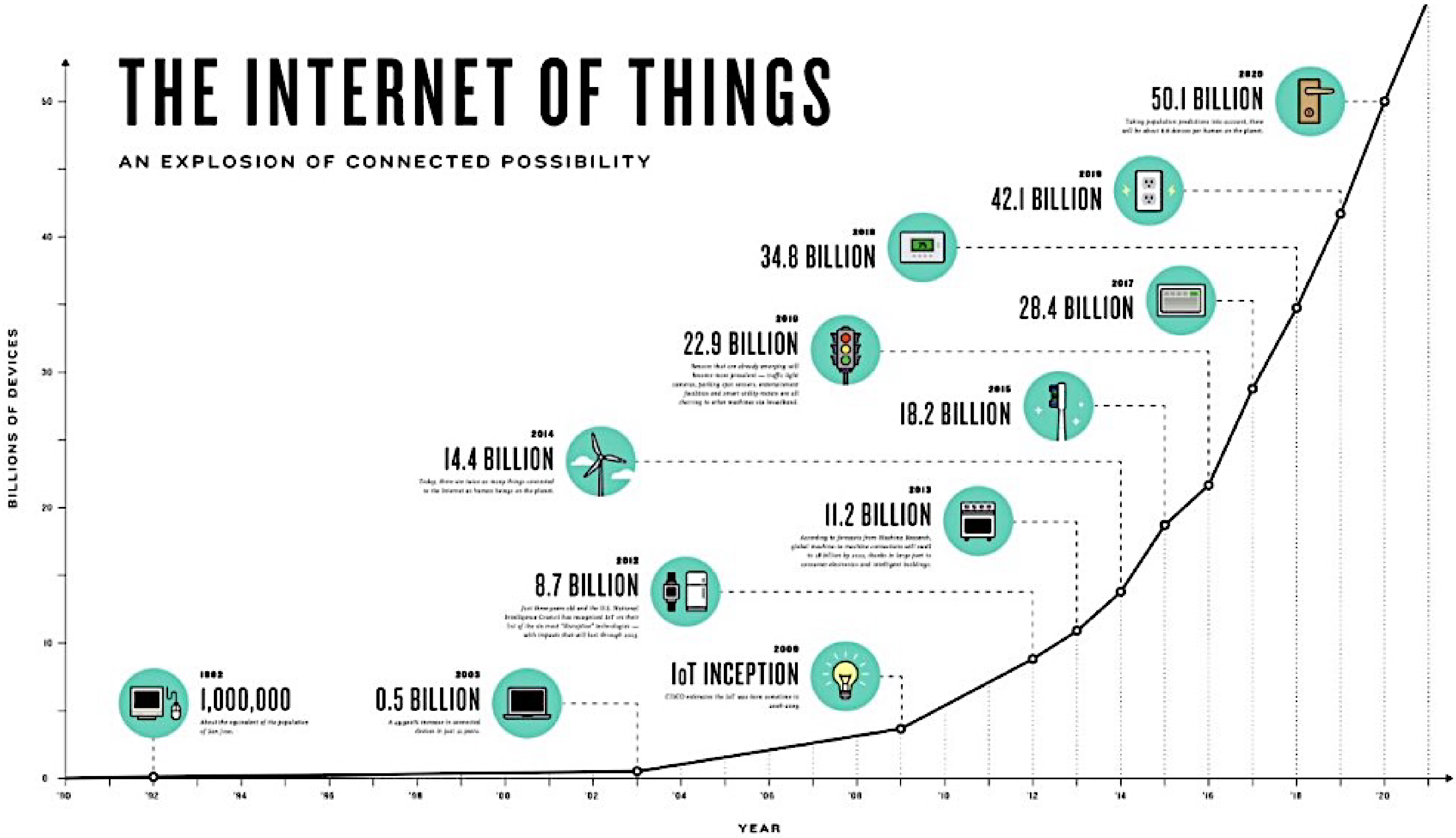
Innovation to Existing Products

Lagging Regulations

Inconsistently Applied “Best Practices” & IoT Standards

THE INTERNET OF THINGS

AN EXPLOSION OF CONNECTED POSSIBILITY



1992
1,000,000
About the equivalent of the population of San Jose.

2003
0.5 BILLION
A 49,900% increase in connected devices in just 11 years.

2009
IoT INCEPTION
CISCO estimates the IoT was born sometime in 2008-2009.

2012
8.7 BILLION
Just three years old and the U.S. National Intelligence Council has recognized IoT on their list of the six most "disruptive" technologies — with impacts that will last through 2025.

2013
11.2 BILLION
According to forecasts from Machina Research, global machine-to-machine connections will swell to 18 billion by 2022, thanks in large part to consumer electronics and intelligent buildings.

2014
14.4 BILLION
Today, there are twice as many things connected to the Internet as human beings on the planet.

2015
18.2 BILLION

2016
22.9 BILLION
Sensors that are already emerging will become more prevalent — traffic light cameras, parking spot sensors, entertainment facilities and smart utility meters are all chattering to other machines via broadband.

2017
28.4 BILLION

2018
34.8 BILLION

2019
42.1 BILLION

2020
50.1 BILLION
Taking population predictions into account, there will be about 6.6 devices per human on the planet.

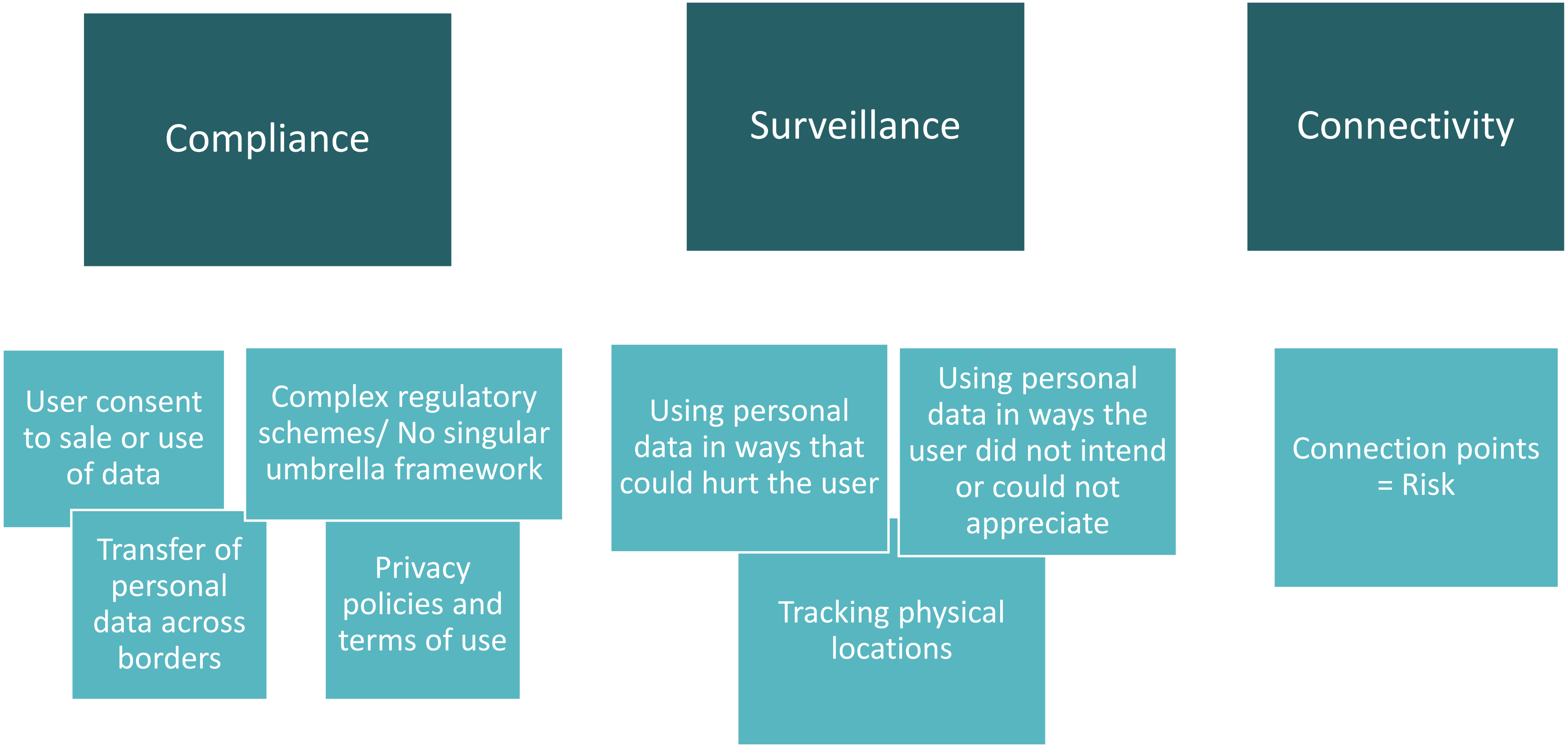
Principal Privacy Concerns

What and Where is Data?

What's the Law?

What's the Risk? Who bears it?

Identifying Scope and Parameters in the Ecosystem



Compliance

User consent to sale or use of data

Complex regulatory schemes/ No singular umbrella framework

Transfer of personal data across borders

Privacy policies and terms of use

Surveillance

Using personal data in ways that could hurt the user

Using personal data in ways the user did not intend or could not appreciate

Tracking physical locations

Connectivity

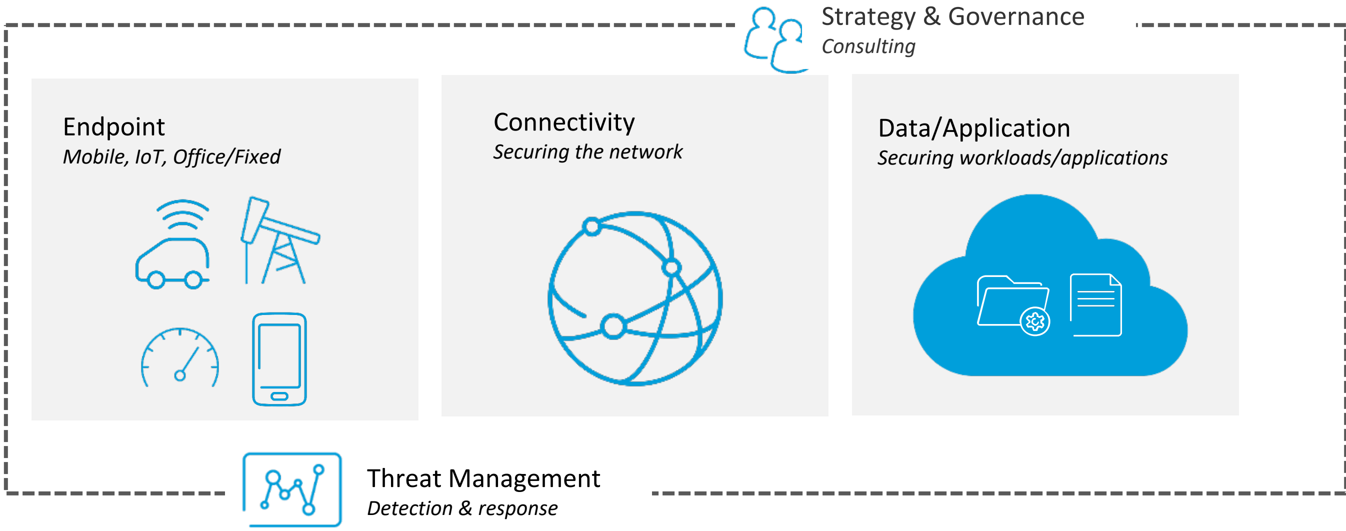
Connection points = Risk

Potter
Anderson
Corroon LLP

Securing the IoT Ecosystem

Top IoT security/privacy concerns

- Device security
- Convergence of OT and IT
- Secure data in transit
- Secure data at rest
- Integrity of the data
- Reliability of the data
- Sustaining operations
- Physical safety
- Operational efficiency
- Access & authentication (devices & users)
- Software/Firmware updates



Strategy & Governance
Consulting

Endpoint
Mobile, IoT, Office/Fixed

Connectivity
Securing the network

Data/Application
Securing workloads/applications

Threat Management
Detection & response

Regulations Impacting Connected Devices

Who's in charge of the IoT?

- Federal and State Laws and Regulations
- Industry standards and industry-wide group regulations
- International / Foreign Laws

= No single governing law to look to …..

Federal and State Privacy Laws

- No broad privacy law (yet) at the federal level
- Silo'ed (industry or business specific) federal laws (GLBA, HIPPA)
  - Various agencies oversight (FTC, FDA, SEC)
- Growing number of broad state privacy laws (CA, VA, UT, CO, CT)
- Growing number of narrow state privacy laws (IL, FL)
- Growing number of state data breach laws (all states now)

Federal and State Privacy Laws

What do these laws intend to protect or cover?

Data Protection – Adhering to consumer wishes with respect to their data

Data Breach – protection of data once the provider has it /has access to it

General consumer rights – transparency and accountability

Federal and State Cyber Security Laws

No single US law

BUT More uniformity in Cyber vs Privacy – through Cyber Security and IoT laws

Federal - Internet of Things (IoT) Cybersecurity Improvement Act of 2020 (“the Act”)

Federal – Cybersecurity Information Sharing Act of 2015

Federal – Various Executive Orders and Agency Rules (SEC)

Federal and State Cyber Security Laws

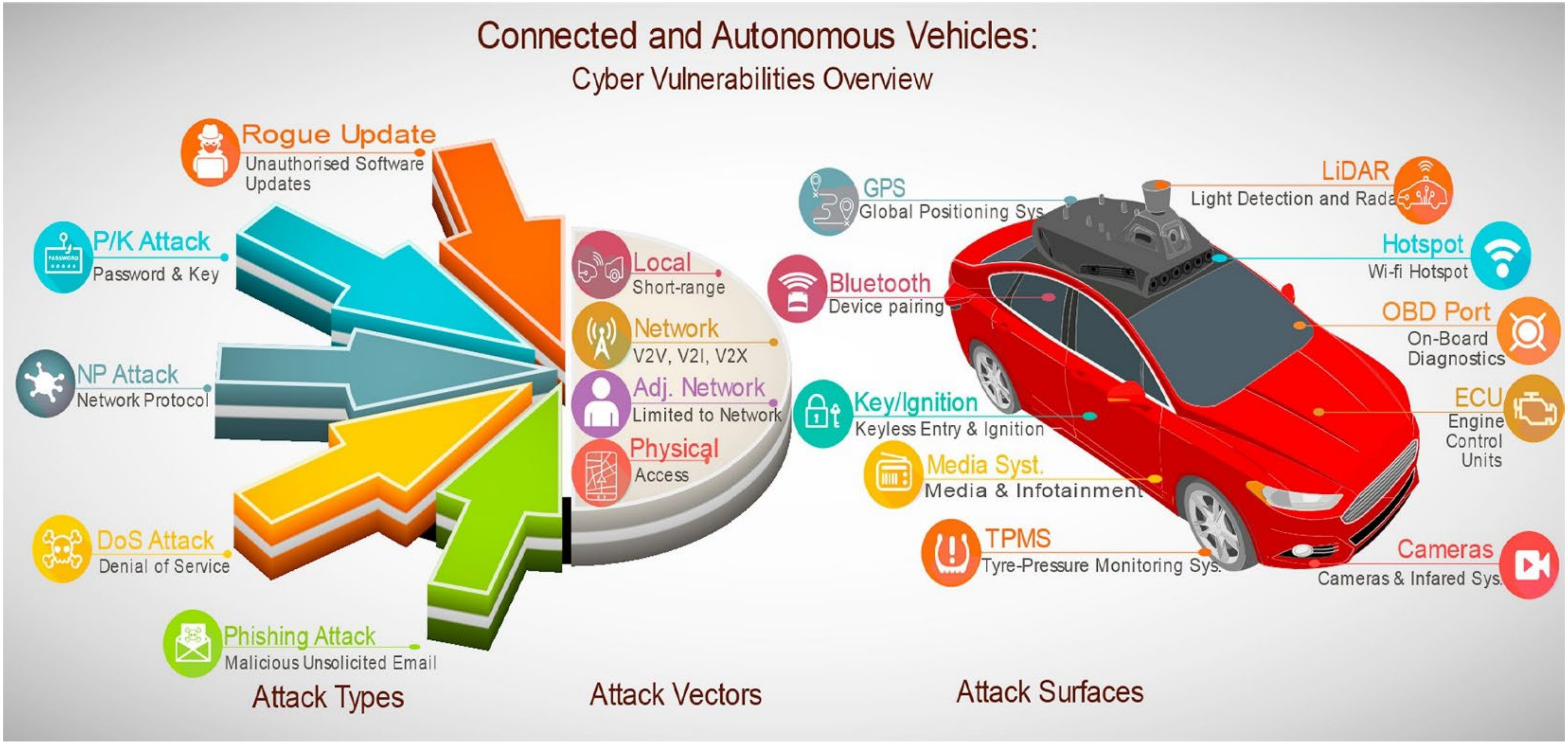
- Focus on financial services industry

California – Internet of Things Security Act Reasonable security measures Authentication

New York – NYDFS Cyber Security Regulation

Practical Examples

Example #1: Connected Vehicles



Potter
Anderson
Corroon LLP

CarsBlues - 2018

- **PRESS RELEASE – 2018 - CarsBlues Vehicle Hack Exploits Vehicle Infotainment Systems Allowing Access to Call Logs, Text Messages and More**
- The hack exploits were discovered by a Remarketer in February 2018.
- Upon discovery, company notified the Automotive Information Sharing and Analysis Center (Auto-ISAC)
- Finder worked for months with Auto-ISAC to help its affected members understand how an attacker might access stored contacts, call logs, text logs, and in some cases even full text messages without the vehicle's owner/user being aware - and without the user's mobile device being connected to the system.
- Updates have been made but there are still issues – according to the researcher, **4 out of 5 cars sold last year contained personal data.**

Industry Assessments

AUTO-ISAC

AUTO-ISAC
Automotive Information Sharing and Analysis Center

2021 Annual Report & Threat Assessment

CONTE

Auto-ISAC 2021 Threat Assessment

7 Key Judgements

Anticipated Threats to the Automotive Industry in 2022
❑ Ransomware Groups
❑ Other Cybercriminal Organizations
❑ State-Sponsored Advanced Persistent Threat Groups
❑ Technology-Enabled Vehicle Theft

- In 2021 there were numerous ransomware and other cybercrime attacks on automotive companies, suppliers, and service providers resulting in disruptions of business and industrial operations and loss of sensitive information.
- Vehicle thefts in the United States decreased significantly (-4%) in 2019 and then spiked nearly 11% in 2020 (when COVID took hold), well above the previous 5-year annual trend (+/- 1-2%). Vehicle theft is expected to remain elevated in the coming year.
- The true scope of global technology-enabled vehicle theft activity is unclear due to lack of metrics on different theft tactics.

AUTO-ISAC 2021 THREAT ASSESSMENT

7 KEY JUDGEMENTS

Anticipated Potential Threats to Connected Vehicles in 2022

- ❑ Malware-Infected Websites, Applications, and Files Accessed via Internet-Connected Devices Synced with In-Vehicle Systems
- ❑ Malicious Exploitation of Vulnerabilities in Information, Communications, and/or Operational Technology
- ❑ Threat Actor use of Nation-State-Quality Cyberweapons

- ➢ **Barring technology-enable vehicle theft, malicious cyberattacks on connected vehicles are not occurring.**
- ➢ **Researchers are finding and reporting connected vehicle vulnerabilities to vehicle manufacturers.**
- ➢ **Proactive imagination of how new and old vulnerabilities, malware, and tools could lead to cyberattacks that threaten vehicle safety will keep the industry ahead of potential threats and the continuously evolving threat environment.**

Q1 Bottom Lines Up Front

Derived from Auto-ISAC DRIVEN, Weekly CAR, RED Platform Alerts, and Partner Reporting

Ransomware groups have targeted at least 26 automotive manufacturers, suppliers, and service providers.

There is no indication that Russia's war on Ukraine has yielded cyberattacks that have adversely impacted automotive IT, OT, or connected vehicle cybersecurity.

Cyber threat actors continue to diversify social engineering tactics, techniques, and procedures to infiltrate business networks and industrial systems.

Notable vulnerabilities in IT, OT, and connected vehicle systems continue to be found.

There have been at least 5 incidents of data leaks resulting from third-party cyber incidents.

Ransomware groups have targeted at least 26 automotive manufacturers, suppliers, and service providers.

Notable Incidents In Q1

- Suspected Conti ransomware compromised 5 auto companies
- Ransomware reportedly not yet deployed in the compromised networks

Impacts

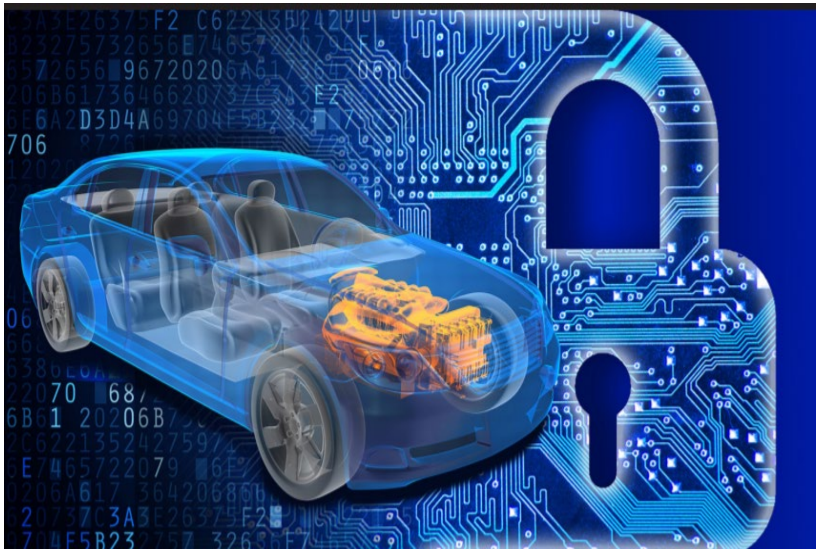
- Network infiltrated by malicious actors
- Customer, employee, and OT information exfiltrated, some sold on the dark web
- 1-day industrial ops shut down
- Business-to-business/ Electronic Data Interchange/ general internet connections shut down
- Dealership commercial activity shut down for days
- No production impacts

Active Groups

- Conti (most active)
- Lockbit 2.0 (2nd-most active)
- Stormous
- Pandora
- AlphaV
- Hive
- Clop
- Kostovite, Petrovite, Erythrite
- BlackCat
- BlackMatter/Darkside
- AvosLocker
- Loki Locker

Standards, Regulations and the Connected Vehicle Ecosystem

- The global connected vehicles continue to grow in numbers
- It is estimate by 2023 there will be nearly 800 million connected vehicles
- A unified approach was needed to address cyber threats across the many stakeholders
- Auto-ISAC built seven (7) Best Practices Guides in 2016
- NHTSA published "Cybersecurity Best Practices for Modern Vehicles" in 2016
- SAE Issues J3061 "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems" (Jan, 2016)



Regulations Impacting Connected Vehicles

- United Nations Economic Commission for Europe (UNECE) WP.29, Cybersecurity; R155, R156
  - Cyber security management system
  - Software update management system
  - Manufacturers will need to **guarantee that their suppliers also implement cybersecurity measures**
- U.S. SELF DRIVE Act
  - Safety and innovation in testing and deployment of autonomous vehicles
  - Cyber security policies for highly automated vehicles
- Federal Trade Commission Act – unfair and deceptive trade practices
- State Data Protection Laws (comprehensive laws passed in 5 states, more coming)
- Emerging Standards
  - ISO/SAE 21434 (Road vehicles — Cybersecurity engineering standards)
  - ISO/SAE 24089 (Software Update Engineering)

UN ECE WP.29 R155 and R156 along with ISO/SAE standard

- **Unified approach needed with needed flexibility to allow for innovation**
- **Focus is on a high level of safety *and security* while creating a uniform terminology across the industry**

- **UN ECE WP.29's two components:**
  1. R155 CSMS – Cybersecurity Management System – Cybersecurity management from ideation through post production | Requires vulnerability management, audit reporting

  1. R156 SUMS – Software Update Management System – Cybersecurity measure to ensure safe software updates through the vehicle lifecycle.

- **US choose not to partake in the UN regulation in the U.S.**

Example #2: IoMT/Digital Health

Combination Of Interconnected Clouds, Technologies, Apps, Devices, Digital Content, And Health Data Used To Deliver Healthcare

- Wearables
- AI diagnostics
- Smart Pills
- Patient identification
- Data Lakes
- Digital Twins
- 5G
- Drones
- Robotics
- Mobile Medical Devices
- Medical Devices
- Telehealth/RPM
- Connected Communities
- Hospitals at Home

Digital Health Remains a Huge Target

- FBI 2021 Cyber Report –
  - Healthcare is #1 in Infrastructure Sectors Victimized by Ransomware
  - Out of 649 attacks, 148 were in healthcare; #2 financial 89
- Verizon: 10 % of data breaches in healthcare
- Experion – “Digital Health: A Blessing and a Curse”
  - Florida Healthy Kids Corporation (3,500,000 health care records exposed),
  - NEC Networks (1.6 million records) and
  - American Anesthesiology (1.2 million records)
  - Hospitals race to keep up with changes in tech

Goals and Challenges of IoMT/Digital Health

GOALS

- Interoperability and connectivity
- Analyze and Use Data to
  - Improve patient outcomes
  - Improve access
  - Improve population health
  - Reduce costs
  - Comply with laws – interoperability
- Innovation

CHALLENGES

- Complex technology, interoperability and connectivity issues
- Cyber and privacy does not keep up with new technologies
- Structured vs non structured data
- Data management and governance
- Algorithms, predictions, AI and Bias
- Vendor Management/Accountability
- Patient/consumer trust

Complex governing laws

- . . . Same Data, Different Obligations?

Covered Entities

- HIPPA/HITECH/Regs - TPO
- FTC (Consumers/Privacy Policies)
- State Data Breach Laws
- Narrow State Privacy Laws
- Standard privacy – TPCA, CAN-SPAM
- Cyber safe harbor– Amendment to HITECH 2021 - NIST

Non-covered entities

- FTC (for Privacy Policies)
- FTC – Healthcare Data Breach Law
- State Data Breach Laws
- Narrow State Privacy Laws
- Standard privacy – TPCA, CANSPAM
- Cyber compliance

FDA, FCC, Other Laws

- FDA - devices, clinical trials
- FCC – drones, 5G
- CISA

Laws on the Horizon

- Bill introduced - Health Data Use and Privacy Commission Act (introduced Feb. 9, 2022)
  - Commission to be tasked with (1) reviewing existing protections of PHI across industries; and (2) making recommendations to update HIPAA to better reflect the use of new digital health and telemedicine technologies.
  - Commission's focus would include:
    - Private-sector activities, including self-regulation efforts
    - Sale of PHI (with or without consent) and the uses of such information
    - Technology advancements for treatment, payment and healthcare operations
    - Non-covered entities, whose data collection and use practices are not covered by HIPAA

Principal Concerns = Potential Contract Issues

When considering the privacy and security concerns in a contract framework, consider:

❑Privity and Parties: Is there a contract that addresses these issues? Who is a party? Consumer/ End User, OEM, Reseller/ Distributor, Third – Party Provider, Unknown

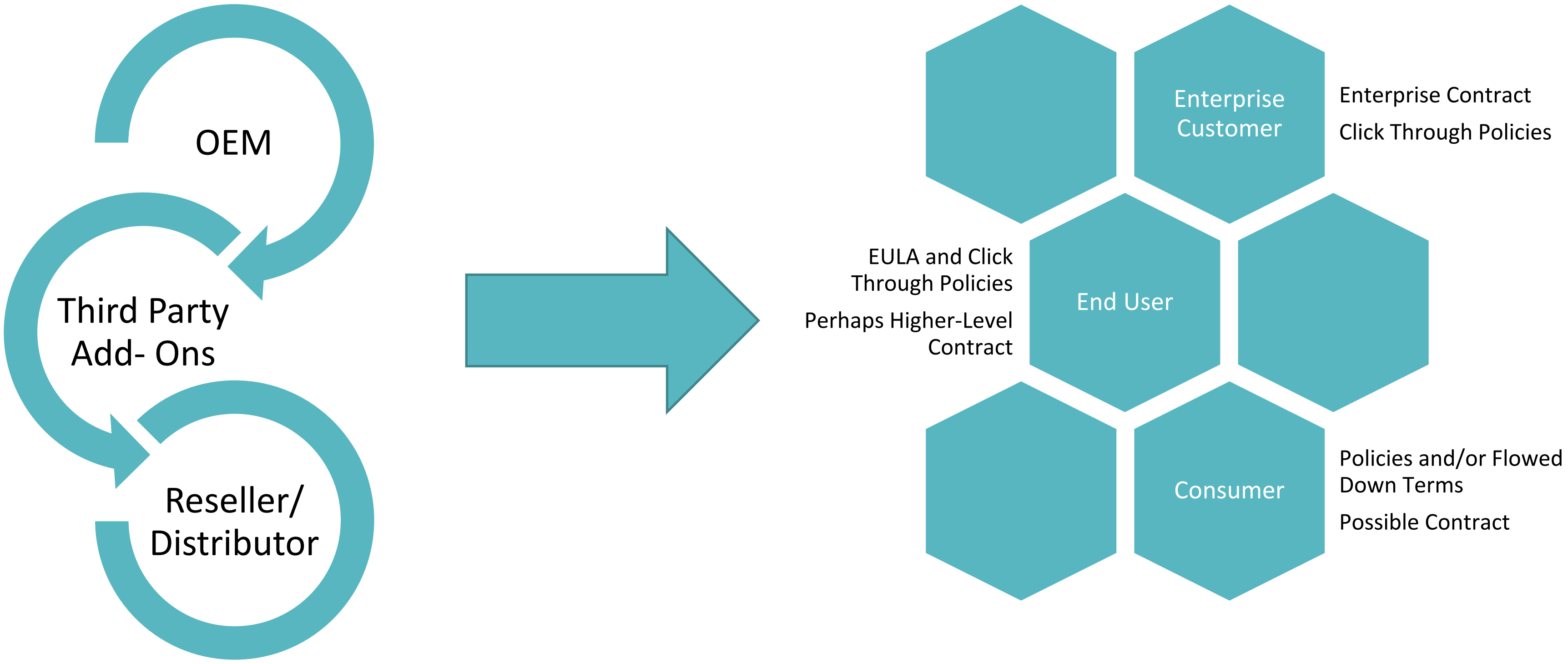
❑Negotiation Power and Form Contracts: Is the contract negotiated or a click through form?

❑Consent: Has the relevant party agreed to the privacy and security standards? Really?

❑Allocation of Risk: As between the two parties, who "should" bear the risk… or who is the better position to bear the risk

❑Regulatory Scheme: What regulatory scheme applies? Does a change in the use or the user affect that answer?

Licensing, Procurement and Supply Chain



OEM

Third Party Add- Ons

Reseller/ Distributor

Enterprise Customer

Enterprise Contract

Click Through Policies

EULA and Click Through Policies

Perhaps Higher-Level Contract

End User

Consumer

Policies and/or Flowed Down Terms

Possible Contract

Best Practices in Procurement

Initial Questions

- Is there a written contract between the parties?
  - What type of contract – license vs. sale?
  - What is the negotiation power? Can parties re-negotiate risk allocation ?
- Are terms being flowed down?
- What policies / click through terms may apply?
- What regulatory framework may apply – and at what which stage of the products' development, sale, and use?

Best Practices in Procurement

Contract Wish List

- Identification of Data and EcoSystem
  - Define “Data”
  - Appropriate language governing ownership
  - Draw a box around the ecosystem – where will data go, how will it be used, who can see / touch data
    - Identify third parties
  - Consider “use” of data and role of legitimate business purpose, analytics, business development/ new product development

Best Practices in Procurement

Contract Wish List

- Protections for Data
  - Covenants requiring compliance with federal and state laws and regulations regarding data security and privacy;
  - Privacy Policy
  - Non-disclosure and confidentiality of information;
    - Includes business / customer / end user/ environmental information
  - Timely notification of application or system changes that will materially affect business or data handling

Best Practices in Procurement

Contract Wish List

- Contractual References to Industry Standards or Regulatory Scheme (or other contractual compliance scheme)
  - Compliance with applicable laws (perhaps other laws?)
  - Compliance with Industry Standards
    - How much effort? How much wiggle room?
  - What are the ramifications for non-compliance and/or breach?

Best Practices in Procurement

Contract Wish List

- Contractual Protections to Ensure Ongoing Monitoring of Vendor Behavior
  - Vendor self-assessments and/or on-site assessments
  - See discussion of notice of testing results and breach/ potential breach
  - Review vendor attestations or certifications
  - Monitor and assess accuracy and quality of vendor's work product;

Best Practices in Procurement

Contract Wish List

- Prepare for the Worst-Case Scenario
  - Notification of data integrity and service failure issues;
  - Notification of cybersecurity events and vendor's efforts to remediate those events;
  - Vendor business continuity planning and practices, including frequency and availability of test results
  - Disclosure of relevant pending or ongoing litigation;
  - Endgame – What happens to the data at the end of relationship?
    - Do not assume friendly break up
    - Ease of transition of key data (if needed); destruction of other data?
    - No holding data for ransom
  - Business and regulator access to books and records

Best Practices in Procurement

Contract Wish List

- Contractual Allocation of Risk
  - Reps and Covenants – triggers for breach (use of materiality and knowledge standards)
  - Use of contractual indemnification rights
  - Role of Insurance to shift risk
  - Remediation
  - Other consequences beyond termination
  - NOTE: Does the regulatory scheme provide for an allocation of risk that the parties wish to deviate from?

Best Practices in Procurement – Contract Key Take Aways

Identify

- **Who Parties Are**
- **What is Data**
- **Where is Data going**
- **Why are people using/ touching it**
- **How can you get it back**

Allocation of Risk

- **Limitations of Liability**
- **Indemnification**
- **Insurance – Cyber, E&O, Business Interruption**
- **Special Provisions – Remediation**

Best Practices – Ongoing

While not required by contract, businesses should:

❑ Be aware of news of vendor deficiencies and investigate whether they indicate a problem with an activity or function the vendor is performing;

❑ Investigate customer complaints that may indicate issues with vendor;

❑ Train staff to address and escalate red flags that a vendor may not be performing an activity or function adequately;

❑ Implement effective technology change management; and

❑ READ THE CONTRACT AND ALL POLICIES.

What Next?

- Predictions for the near future
  - Role of rules and regulations?
  - How fast can regulators and industry self-regulators move?
  - How important is supply chain visibility control?

Highlights for the IoMT/Digital Health Area:

- Increase In Healthcare Vulnerability through Supply Chain Cyber Attacks
- Increase in regulatory focus on healthcare vendors – especially non-HIPAA
- Increase in Patient And Consumer Rights
- Increase in FTC examination of compliance/privacy policies
- Race to Build More Secure Data Sharing and Management - Amazon, Google, Apple – Creative Big Players

Contact Us

William R. Denny
Direct dial: (302) 984-6039
wdenny@potteranderson.com

Potter Anderson & Corroon LLP
1313 North Market Street
Wilmington, DE 19801

potteranderson.com