RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: GRC-R01

Managing the Unmanageable: A Risk Model for the Internet of Things

Gib Sorebo

Chief Cybersecurity Technologist
Leidos
@gibsorebo

What is the Internet of Things?

"The Internet of Things (IoT) is still somewhat of a vague concept and carries a number of definitions. The IoT in general refers to an Internet-like structure that connects uniquely identifiable objects, basically anything that can be tagged with an identifying chip. The "things" in the network take on virtual representations, and can interact with each other as well as gather data such as when and how objects are being used, their operating condition, etc."

http://www.csoonline.com/article/2134066/mobile-security/what-the-internet-of-things-means-for-security.html

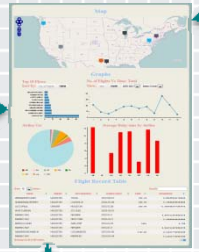
- Does is it have to be connected to the Internet or even have an IP address?
- Interact only with other "things" (i.e., machine-to-machine) or can people be involved?
- Cynics would argue that IoT is an "invention" that's been in existence for decades

Useful to Think in Terms of Overall Process

Collection (sensors, cameras, meters, GPS, measure glucose level)

IoT Support Functions

Analysis (ingest, sort, transform, calculate)



Decisions (likely human interface, smart agents, triggers, decision support systems)

Core IoT Areas

Action (actuators, drones, self-driving cars, pacemaker shocks, supply insulin)

Case Study: The “Uber” of the Future

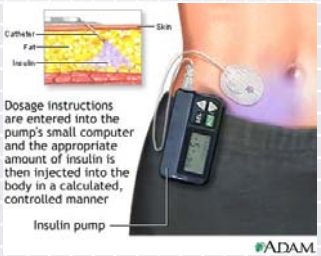
Vehicle reports GPS position, cost data, charging status, etc.

Data on all cars is aggregated and sorted to deliver to customers

Customer selects vehicle and designated route with payment data on file and car is requested

Car receives request and autonomously travels to customer for pickup for arranged travel

The Threats are Real and Growing….



Insulin Pumps (2013)

Car Washes (2015)

Stuxnet (2010)

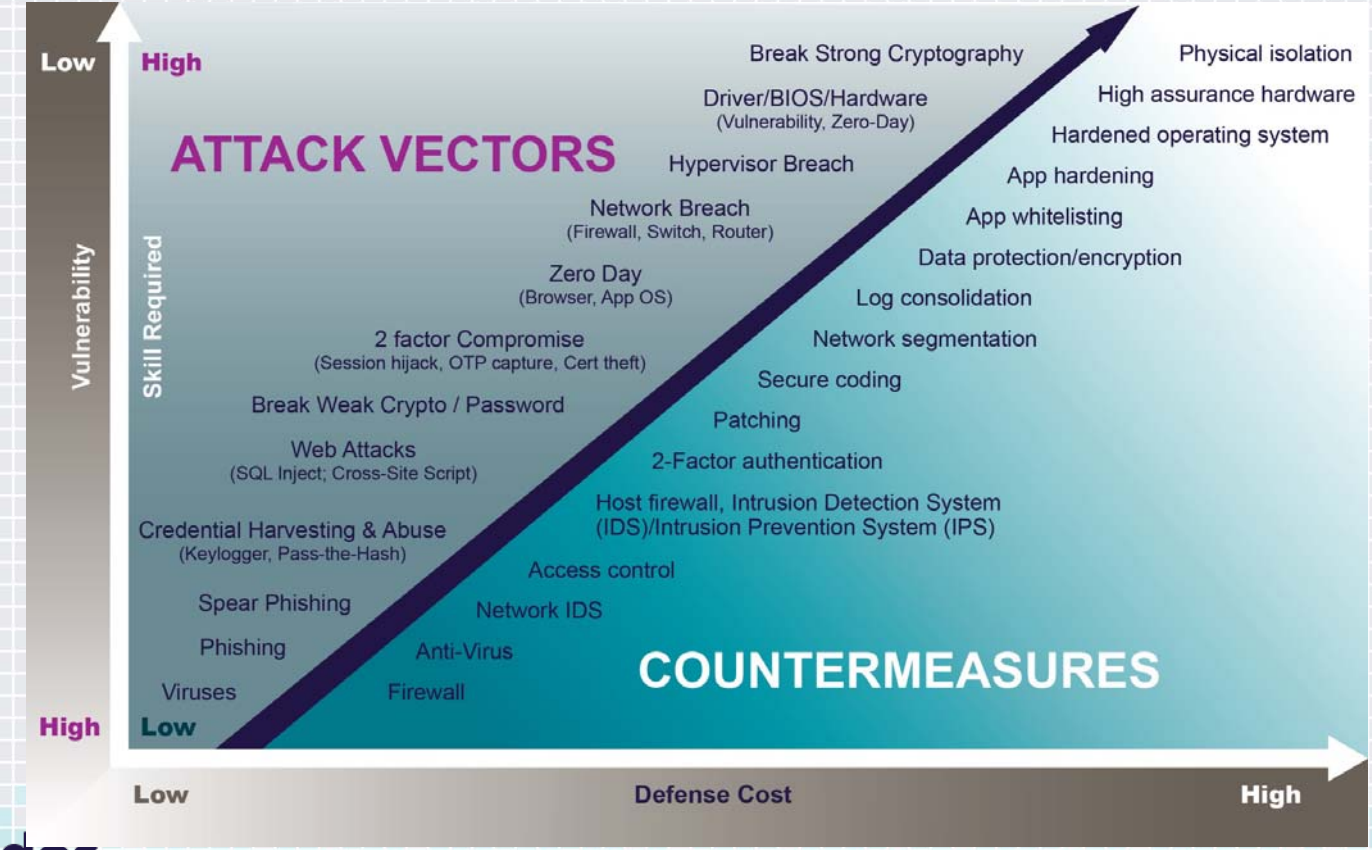
German Steel Mill (2014)

Federal Energy Regulatory Image. Used by permission.

Taum Sauk (2005)

But the Devices and Risks are Diverse…so How Do We Secure Them?

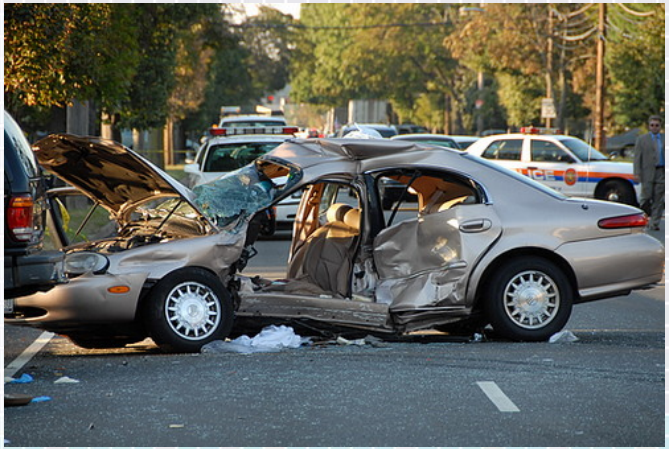
One Way: Look at the Threat and Pair with Appropriate Controls



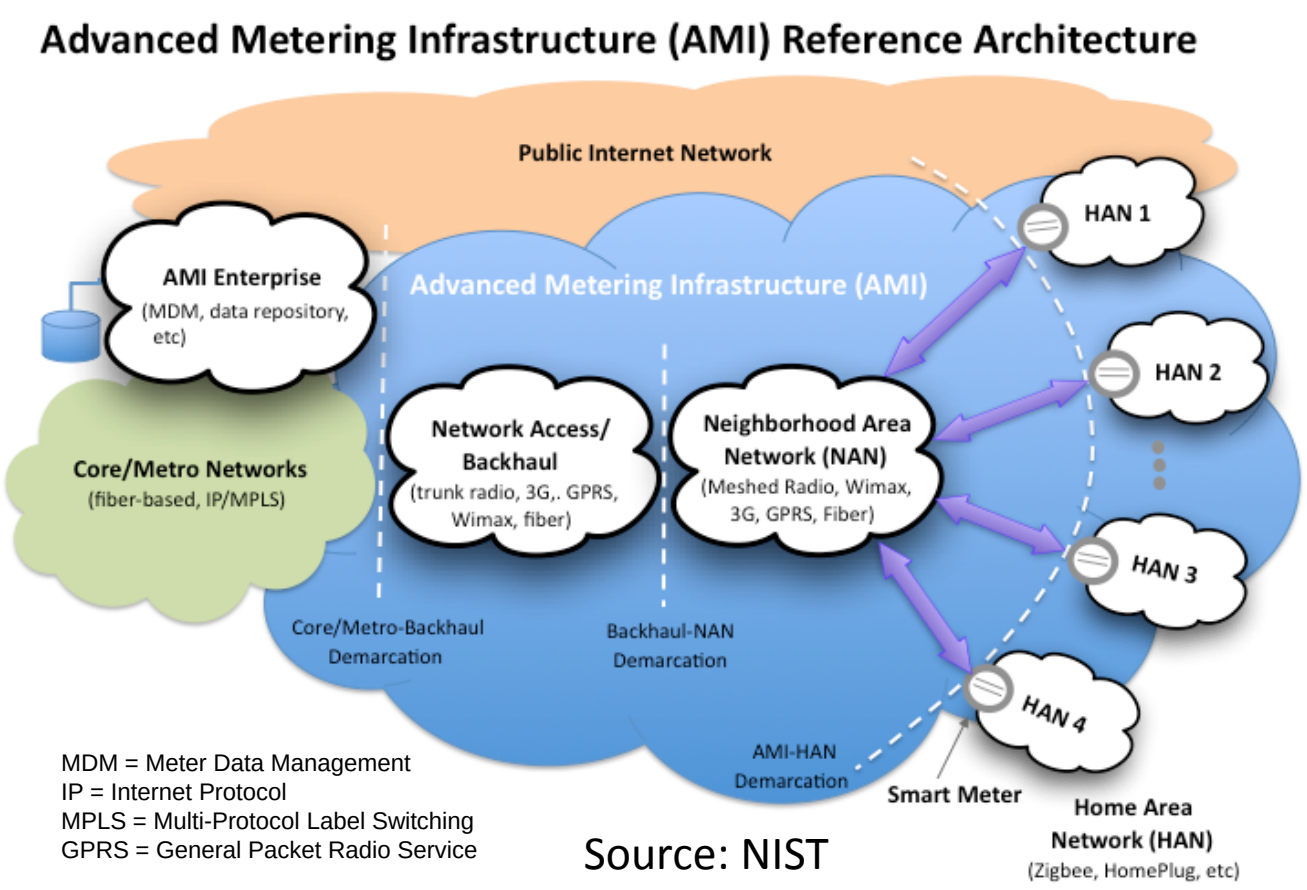
Or Focus on the Impacts

U.S. Homeland Security photo

U.S. Geological Survey, USGS/Rolla, Mo.
Used by permission.



Case Study: Smart Metering



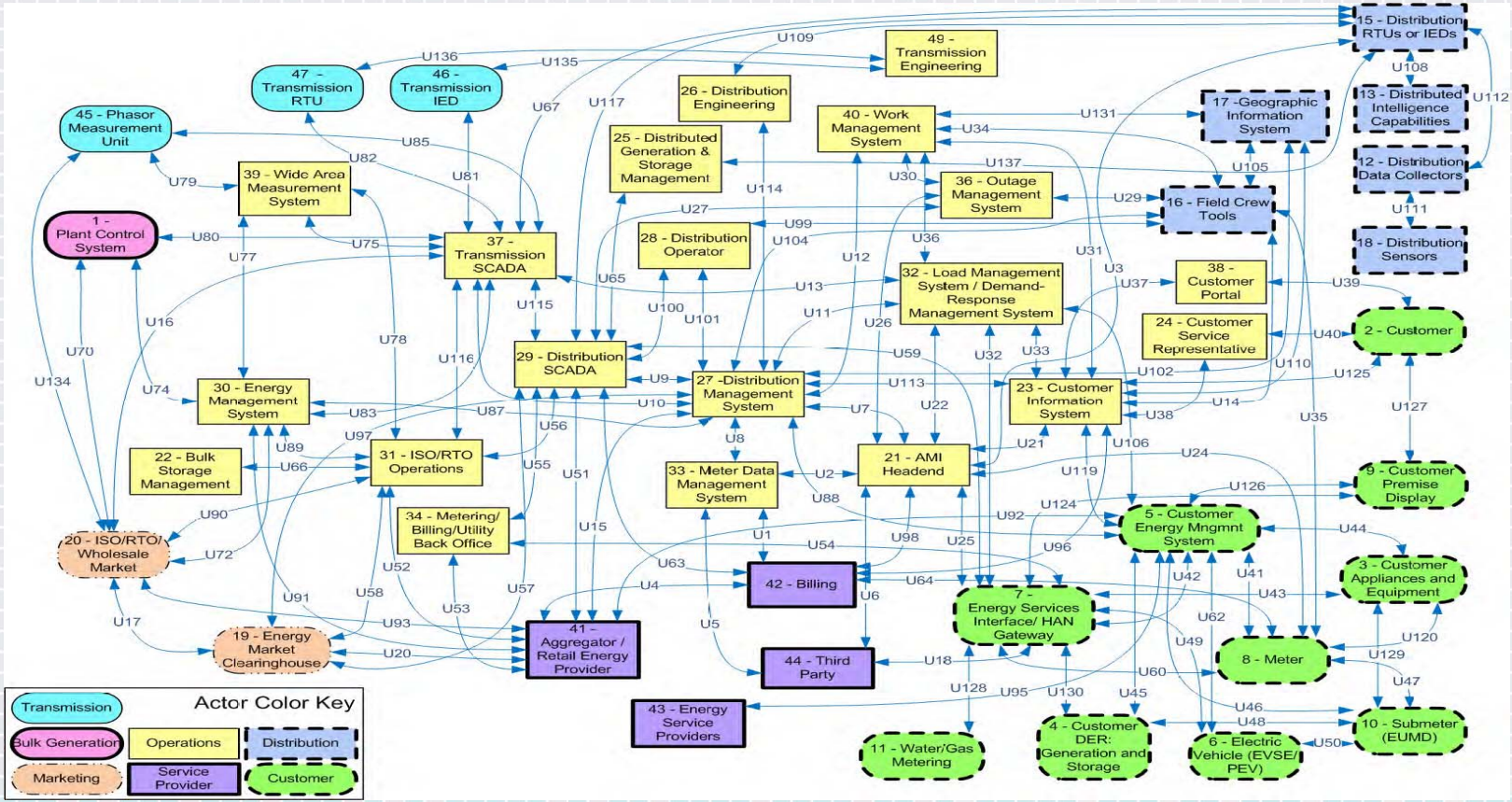
MDM = Meter Data Management
IP = Internet Protocol
MPLS = Multi-Protocol Label Switching
GPRS = General Packet Radio Service

Source: NIST

Typical Use Cases

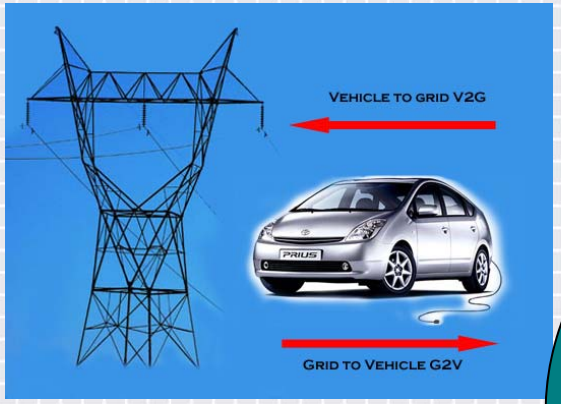
- Identify outages
- Billing
- Reduce energy theft
- Detect voltage drops
- Remote connect / disconnect
- Demand response
- Customer education
- Marketing data

But It Can Get Complicated (Smart Grid Interfaces)



Source: NIST

Need to Anticipate Future Use (and Abuse) Cases



…and energy theft

Home automation
… and stalking

Vehicle to vehicle communication
…. and road rage hacking

Case Study: Privacy …. A Slippery Slope

Intelligent TVs

Data Granularity

Data Aggregation

Device Convergence

Seemingly Innocuous to Potentially Insidious

leidos

Building the Risk Model

Define Use Case

- Be as specific as possible
- Identify all components
- Note business objectives
- Create use case for each variation
- The “devil will be in the details”

Identify all relevant impacts

- Start with the worst thing that can happen (e.g., loss of life)
- Make sure you include all relevant externalities (e.g., what would consumers or regulators think?)

Likely vulnerabilities

- Start with all interfaces and potential attack surfaces including physical access
- May need to stay in the realm of what is reasonably foreseeable
- Make sure these are pared with impacts (i.e., certain vulnerabilities lead to certain impacts)

Identify threats

- Don’t go overboard here
- Many threats have yet to materialize and are very speculative
- Use threats to help with impacts and vulnerabilities
- Threats will evolve significantly as incentives change and IoT becomes more common

Other Considerations

Externalities

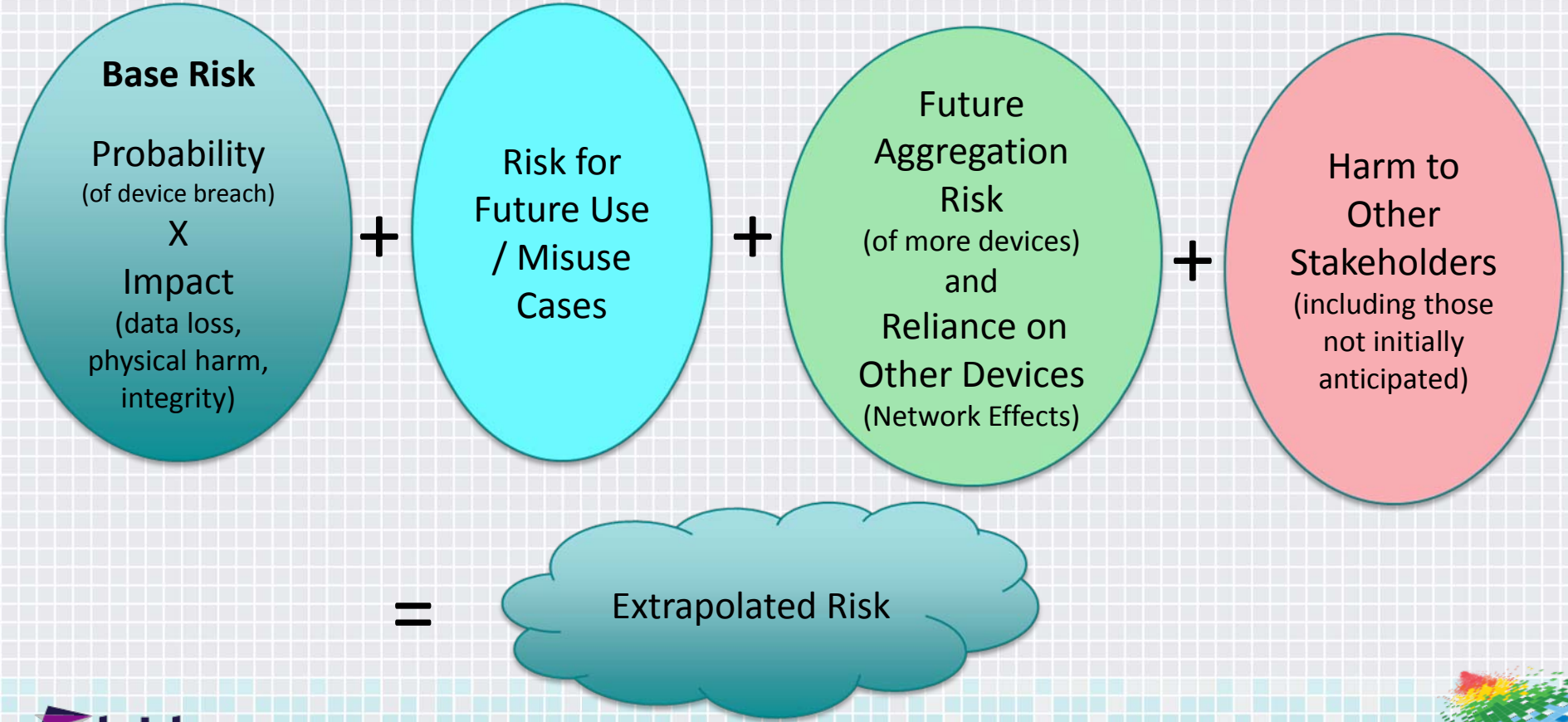
- Device owner or data custodian don't always feel the bulk of the impact
- Reputational harm only goes so far
- Regulation should focus on where the harm occurs

Iterate risk model for each

Typical Stakeholders

- Data subjects
- Those using the devices (possible physical harm)
- Public at-large / community
- Device owners
- Data custodians
- Regulators (local, state, national, global)

Internet of Things Risk Formula



Industry Options for Mitigating Risk

- Fit for purpose
  - Sharply restrict use to only a particular applications, disclaiming liability (or making other uses illegal) for all else (e.g., drone only meant for agriculture observation in unpopulated areas)
  - Generally unrealistic given tendency for usage to expand
  - May actually incur more liability
- Clearly document assumptions for device and its limitations
- Provide for close oversight where devices of different owners interact (e.g., vehicle to vehicle communications, adding energy resources to electric grid)
- Mandate vetted protocols and software libraries for devices that could involve human injury (particularly members of the general public)
- Implement device certification for particular use cases (e.g., safety, large amount of personal information, critical infrastructure)

Organization/Consumer Options for Mitigating Risk

- Detailed use case development
  - Be clear on the permissible uses (e.g., never use in control system environment)
  - Document data collection and retention policies
  - Assign oversight responsibility for each use case and involve people outside of IT
- Review insurance coverage and applicability
- Where possible, implement ongoing security monitoring
- Schedule ongoing reviews of Internet of Things implementation company-wide and for each use case (this includes any new use of data collected)
- Revise risk management model and obtain necessary approvals after each change of scope (and you better believe that scope will change frequently)

Apply What You've Learned Today

- Next week you should:
  - Begin to identify all current Internet of Things implementations that are in place, planned, or anticipated
  - Identify any security policies or procedures related to Internet of Things
- In the next three months you should:
  - Device owners should apply the risk model described and review results with management
  - Identify mitigation steps and associated costs to achieve desired state
- In the next six months you should:
  - Identify Internet of Things risks that you don't control that affect your organization
  - Participate in industry groups to encourage development of security standards for the devices that most affect you

Keys for Successful Internet of Things Security Strategy

Questions?

Thank You.

Gib Sorebo

Chief Cybersecurity Technologist

tel: 703-676-0269 | *email:* sorebog@leidos.com