

Internet of Things (IoT)

Standards, Risks, & Why we Need to Address Both

November 7, 2017

mariner 
SECURITY SOLUTIONS

Anthony English

VP/CISO

CISSP, CIPP/C, ISO27001 Master, CISM, CISA, CGEIT,
ISO27033 Lead Cybersecurity Manager, MCSE, CRISC, HiTrust Certified Practitioner

mariner 
SECURITY SOLUTIONS



IoT – what is it?

Protect Revenue, Assist Governance and Ensure Business Continuity



IoT – what is it?

Protect Revenue, Assist Governance and Ensure Business Continuity

Endpoint Devices

- Cars, farm resources, medical devices, smart TV's, etc.
- Buildings, Infrastructure, Utilities (although typically SCADA)



Gateways

- Short range communication devices such as routers using 802.x, Bluetooth, etc.
- Link from end devices to external networks



Telecomms / Internet links

- Cellular, Fiber, Dedicated links, etc.
- Link gateways to the service level



Service Level

- End user, Big Data, Automation, etc.



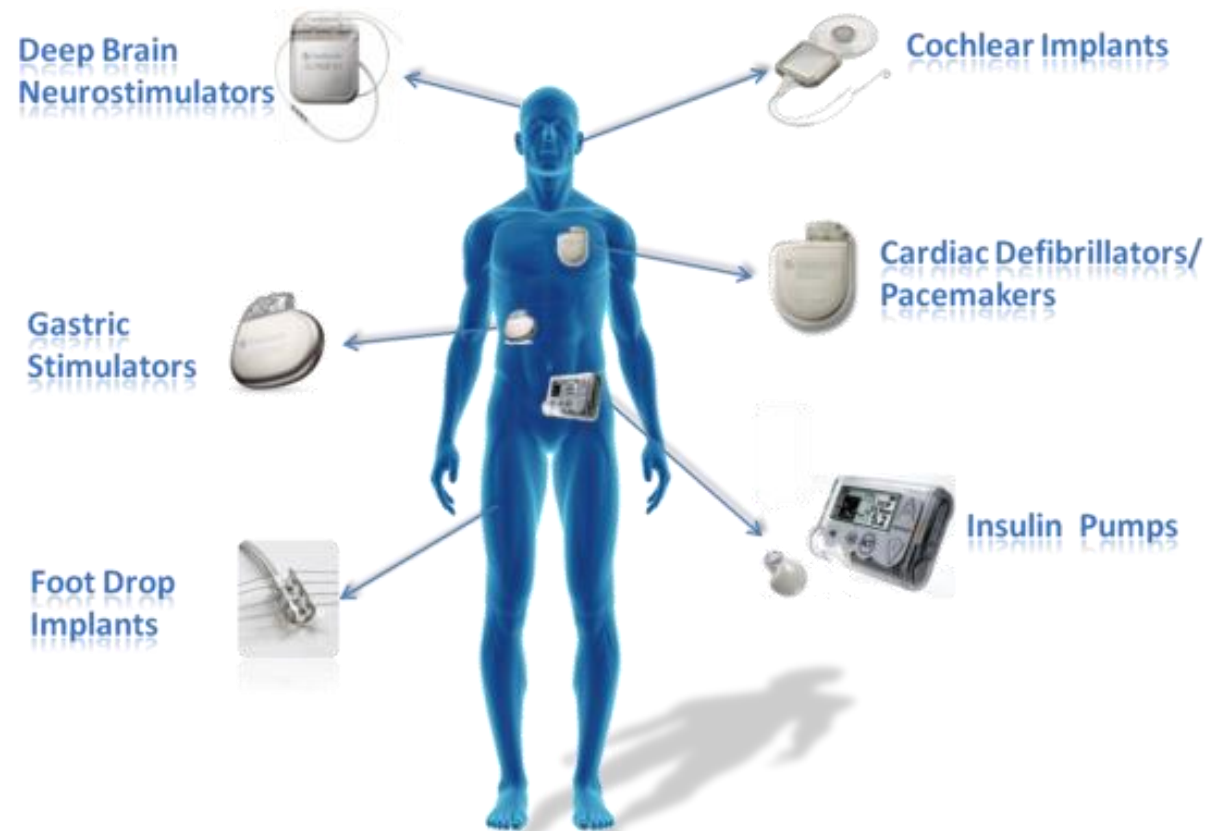
IoT – Where is it?

mariner 
SECURITY SOLUTIONS

IoT – Medical

Protect Revenue, Assist Governance and Ensure Business Continuity

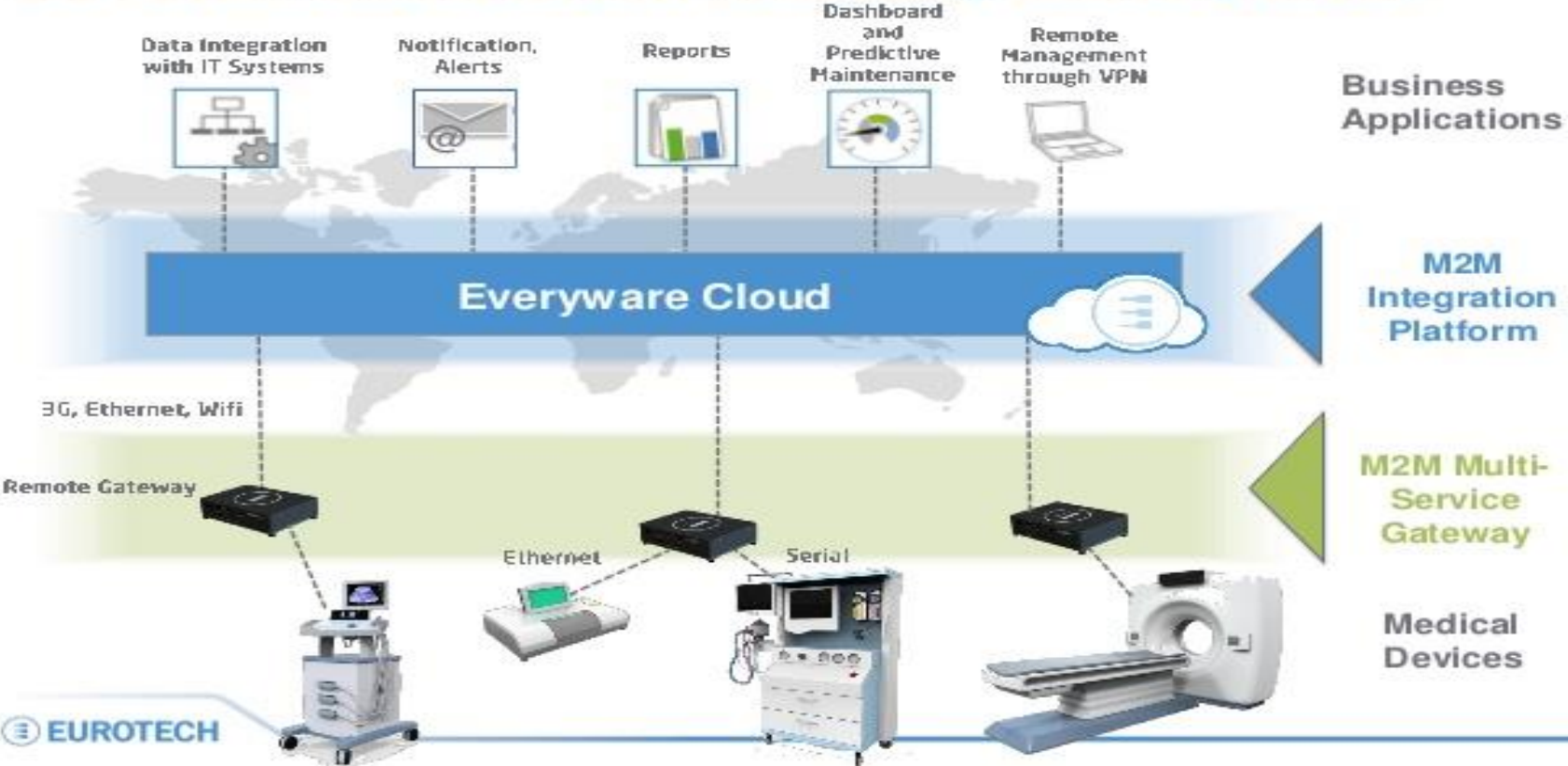
WIRELESS IMPLANTABLE MEDICAL DEVICES



IoT – Medical

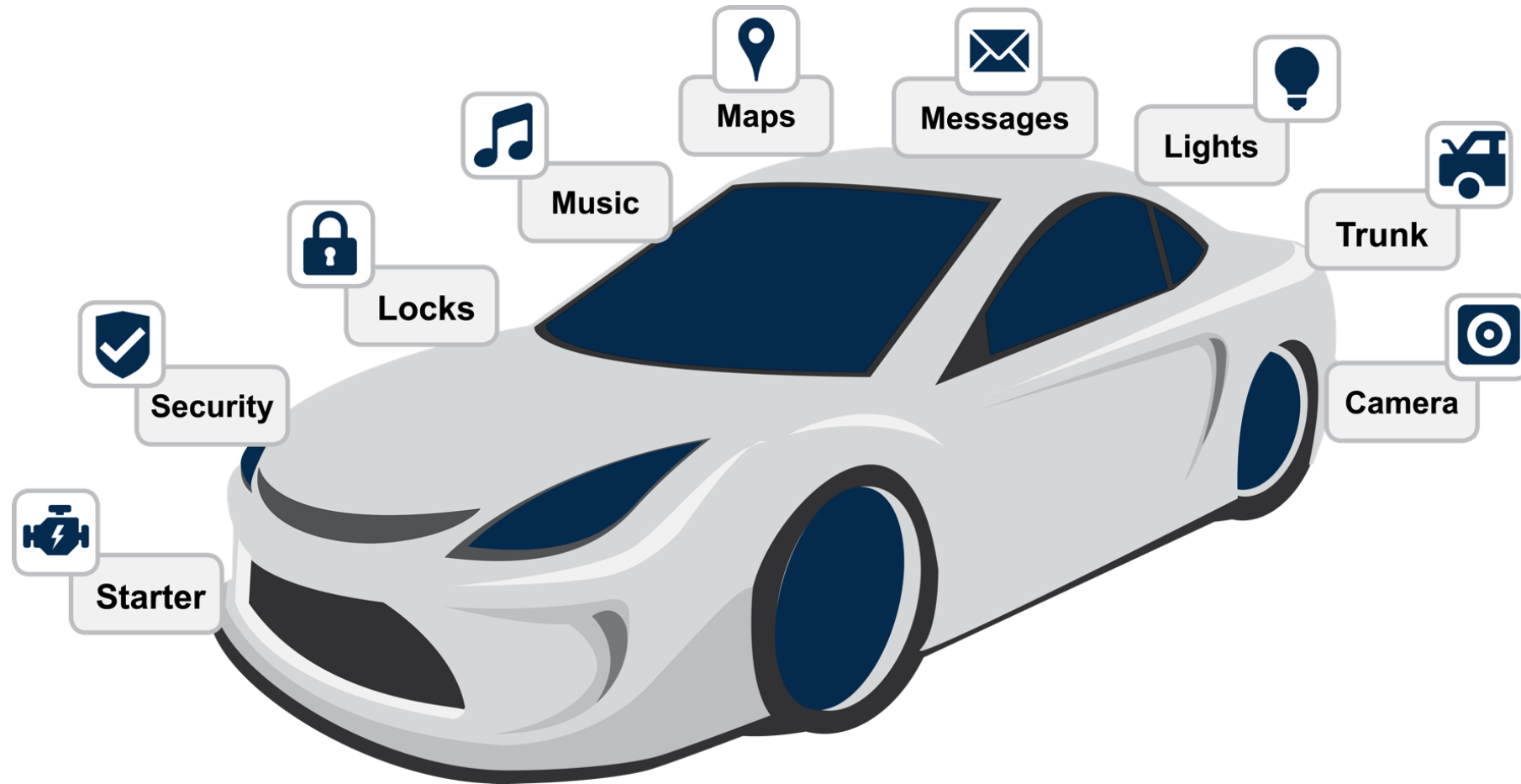
Protect Revenue, Assist Governance and Ensure Business Continuity

Medical & Healthcare IoT Applications Use Case: Remote Device Monitoring & Management



IoT – Automotive

Protect Revenue, Assist Governance and Ensure Business Continuity



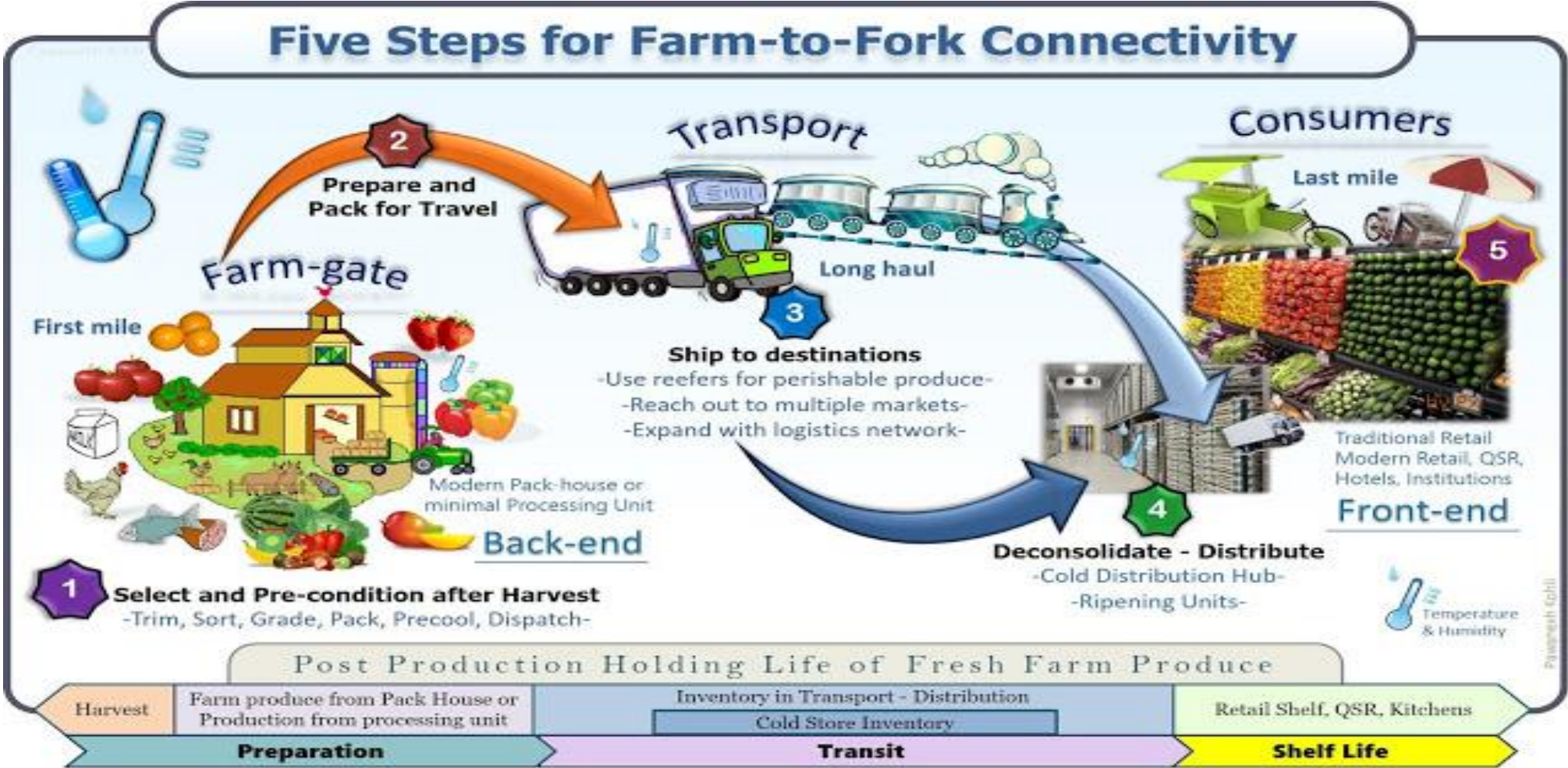
IoT – Smart Cities

Protect Revenue, Assist Governance and Ensure Business Continuity



IoT – Food Supply

Protect Revenue, Assist Governance and Ensure Business Continuity



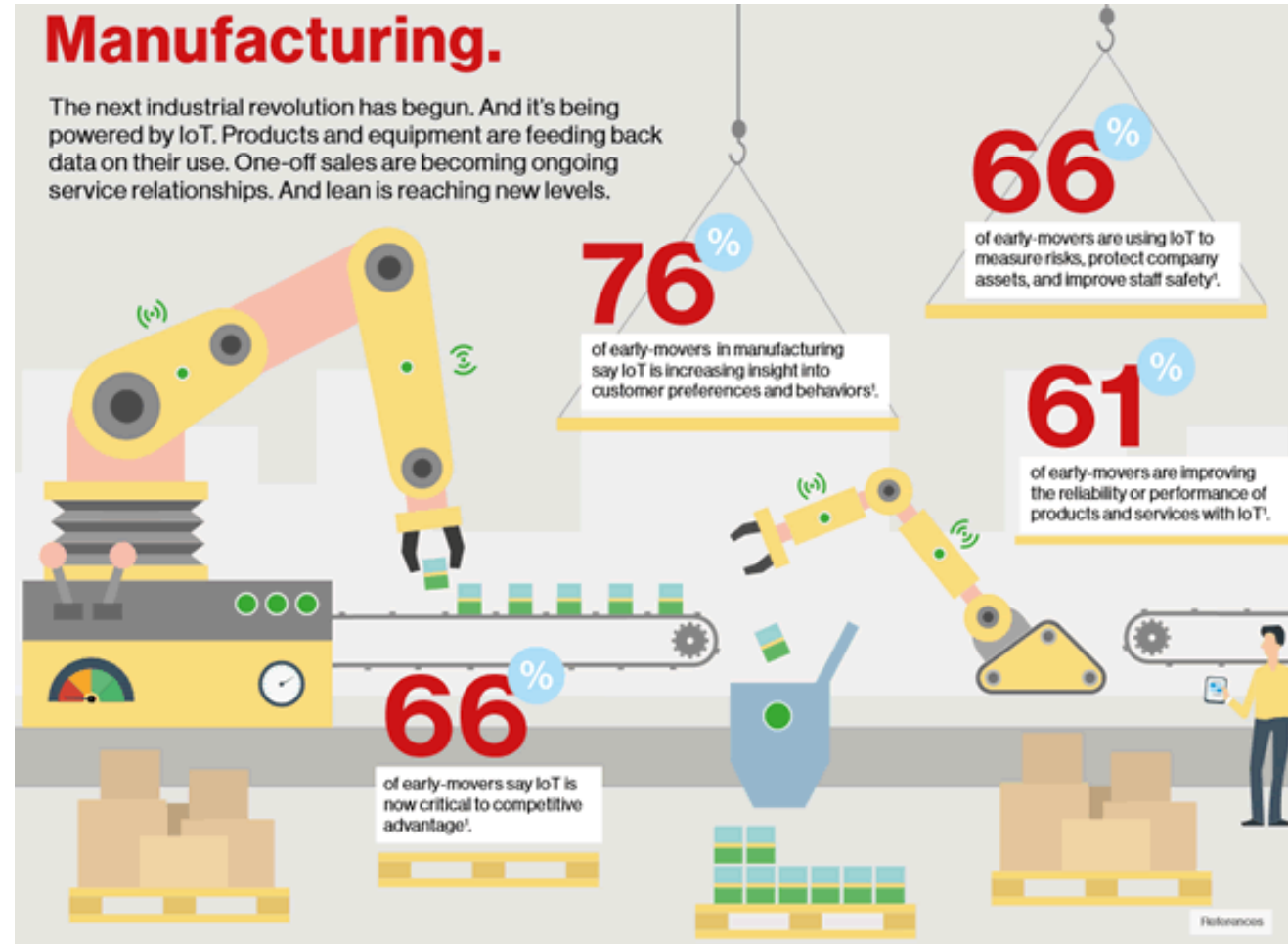
IoT – Utilities

Protect Revenue, Assist Governance and Ensure Business Continuity



IoT – Manufacturing

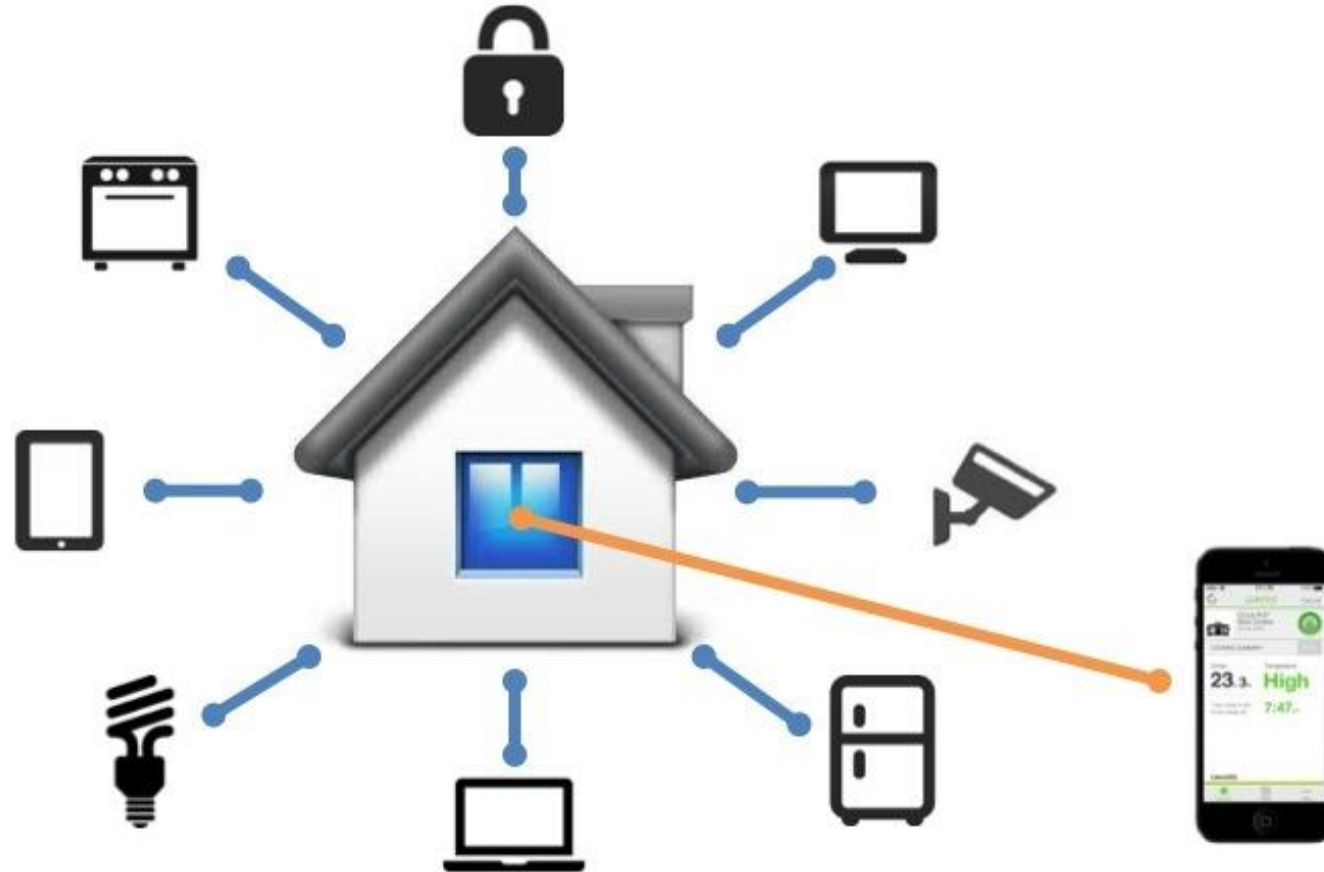
Protect Revenue, Assist Governance and Ensure Business Continuity



*Source: Verizon

IoT – At Home

Protect Revenue, Assist Governance and Ensure Business Continuity



IoT Internals

mariner 
SECURITY SOLUTIONS

IoT – What is the Operating System?

Protect Revenue, Assist Governance and Ensure Business Continuity



IoT Devices – What else is unique?

Protect Revenue, Assist Governance and Ensure Business Continuity



IoT Risks

mariner 
SECURITY SOLUTIONS

IoT – So why worry?

Protect Revenue, Assist Governance and Ensure Business Continuity





Ad closed by Google

Stop seeing this ad Why this ad? ▾

New Rapidly-Growing IoT Botnet Threatens to Take Down the Internet

Friday, October 20, 2017 Wang Wei

Tweet Share 55 Share 1.34k Share 3.13k Share



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

October 17, 2017

Alert Number
I-101717a-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

COMMON INTERNET OF THINGS DEVICES MAY EXPOSE CONSUMERS TO CYBER EXPLOITATION

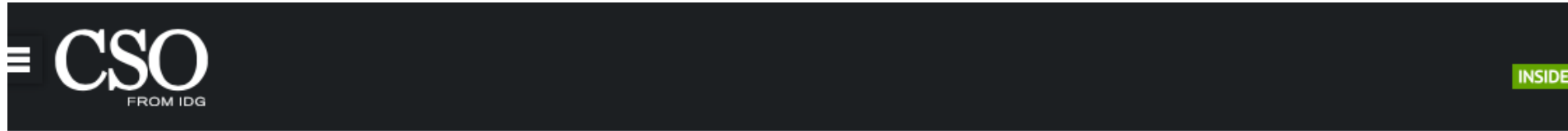
In conjunction with National Cyber Security Awareness Month, the FBI is reiterating the growing concern of cyber criminals targeting unsecure Internet of Things (IoT) devices. The number of IoT devices in use is expected to increase from 5 billion in 2016 to an estimated 20 to 50 billion by 2020. Once an IoT device is compromised, cyber criminals can facilitate attacks on other systems or networks, send spam e-mails, steal personal information, interfere with physical safety, and leverage compromised devices for participation in distributed denial of service (DDoS) attacks.

IoT refers to a network of physical devices, vehicles, buildings, and other



IoT – So why worry?

Protect Revenue, Assist Governance and Ensure Business Continuity



proofpoint.

The Hidden Costs of Microsoft Office 365 Security & Compliance

EXPAND ▾

[Home](#) > [Hacking](#)



PRIVACY AND SECURITY FANATIC

By [Ms. Smith, CSO](#) | SEP 4, 2017 10:04 AM PT

About

Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

NEWS

465,000 Abbott pacemakers vulnerable to hacking, need a firmware fix

The FDA and Homeland Security issued alerts about vulnerabilities in Abbott [formerly St. Jude Medical] pacemakers and a firmware update to close those security holes.



IoT Protocols and Frameworks

mariner 
SECURITY SOLUTIONS

The background features a glowing blue globe with a complex network of white and light blue lines and nodes, representing a global IoT network. The lines are curved and connect various points across the globe, creating a sense of dynamic connectivity.

IoT – Protocols and Frameworks

Protect Revenue, Assist Governance and Ensure Business Continuity

The following is a list of some of the protocols used by IoT:

- 1) Infrastructure – RPL, IPv4/IPv6, 6LowPAN
- 2) Identification – EPC, URIs, IPv6
- 3) Comms/Transport – Bluetooth, LPWAN, WiFi
- 4) Discovery – DNS-SD, mDNS
- 5) Data Protocols – Websocket, AMQP, CoAP, MQTT
- 6) Device Management – OMA_DM, TR-069
- 7) Semantic – JSON-LD
- 8) Multi-layer Frameworks – Weave, Homekit, IoTivity

IoT – Protocols and Frameworks

Protect Revenue, Assist Governance and Ensure Business Continuity

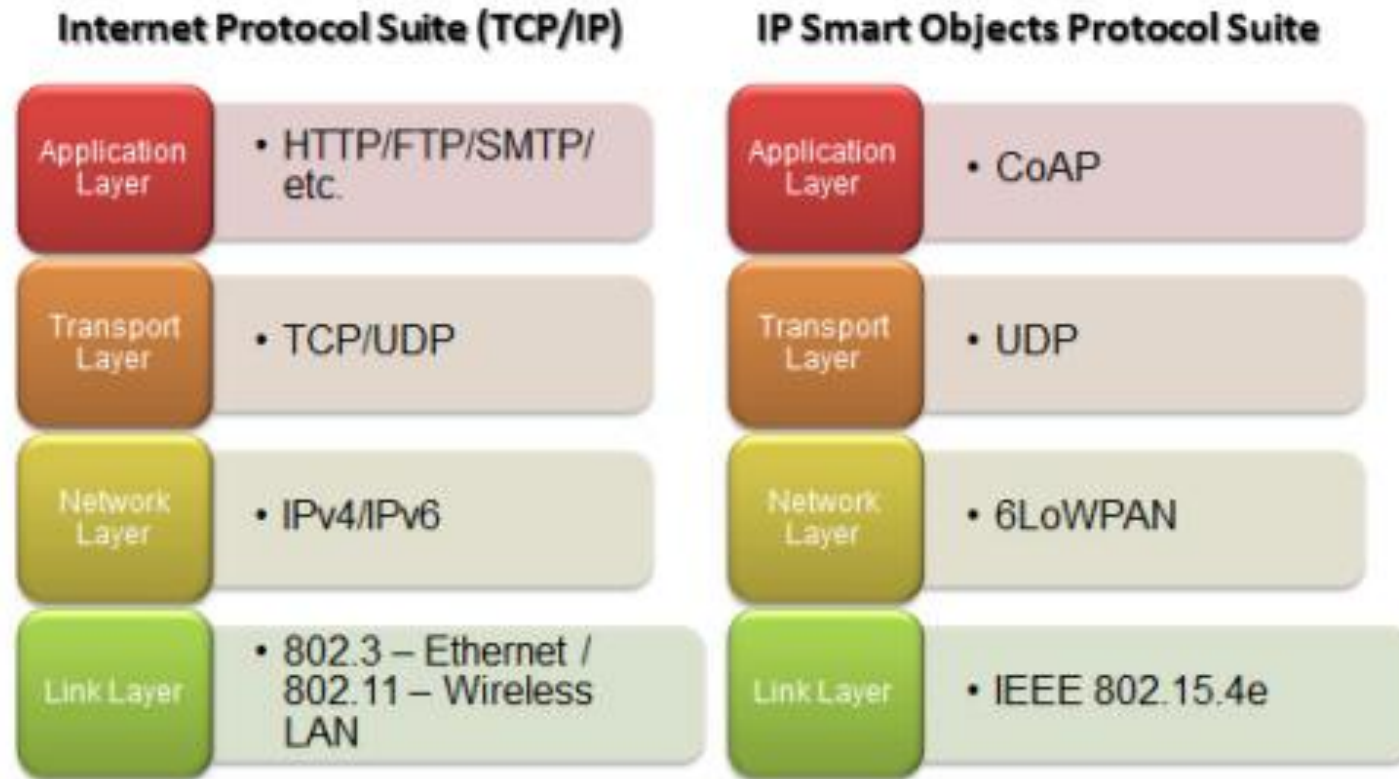


Figure 1 TCP/IP Stack and IP Smart Objects Protocol Stack

*Image from Mindtree Labs.

IoT – Protocols and Frameworks

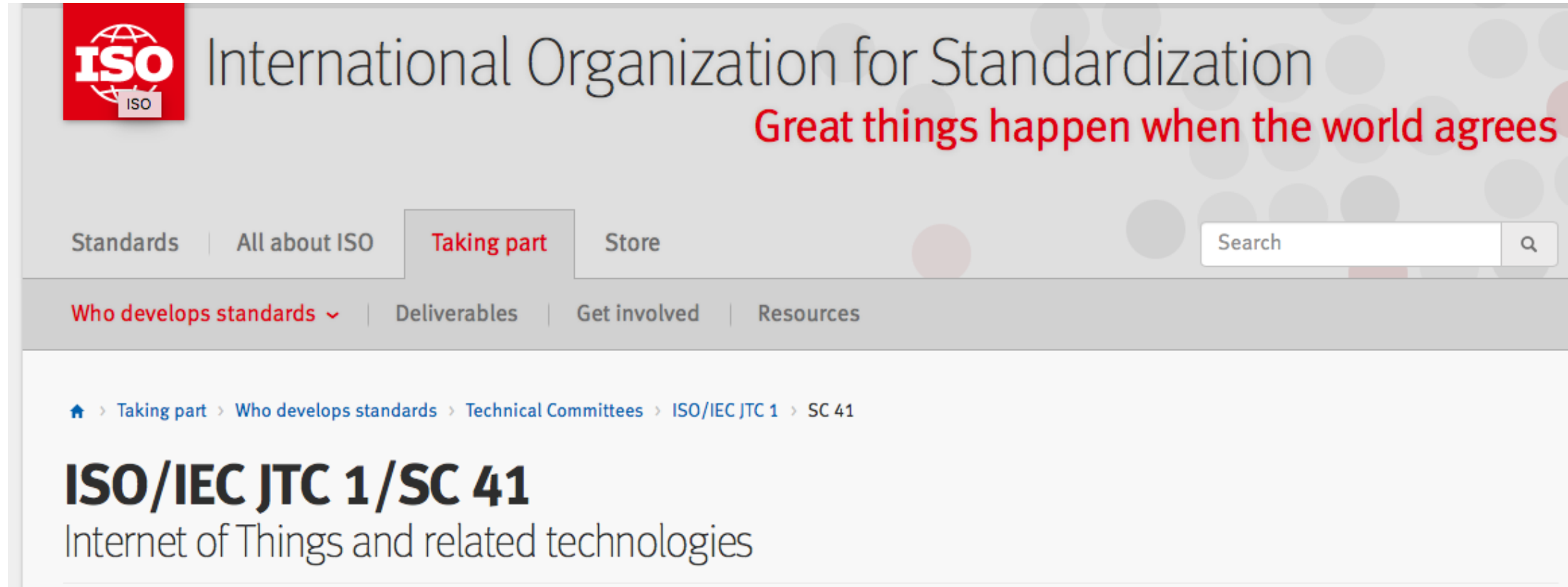
Protect Revenue, Assist Governance and Ensure Business Continuity

OWASP Internet of Things Project



IoT – Protocols and Frameworks

Protect Revenue, Assist Governance and Ensure Business Continuity



The screenshot shows the ISO website header with the ISO logo and the text "International Organization for Standardization" and "Great things happen when the world agrees". The navigation menu includes "Standards", "All about ISO", "Taking part", and "Store". A search bar is located on the right. Below the navigation menu, there are links for "Who develops standards", "Deliverables", "Get involved", and "Resources". The breadcrumb trail is: Home > Taking part > Who develops standards > Technical Committees > ISO/IEC JTC 1 > SC 41. The main heading is "ISO/IEC JTC 1/SC 41" with the subtitle "Internet of Things and related technologies".



IoT – Protocols and Frameworks

Protect Revenue, Assist Governance and Ensure Business Continuity

The screenshot shows the top portion of the NIST website. At the top left is the NIST logo. To the right is a search bar labeled "Search NIST" with a magnifying glass icon, and a "NIST MENU" button with a hamburger icon. Below the search bar is a dark blue bar with the text "Information Technology Laboratory". Underneath that is a light blue bar with the text "APPLIED CYBERSECURITY DIVISION".

Programs



NIST initiatives in IoT

Staff



IoT – Protocols and Frameworks

Protect Revenue, Assist Governance and Ensure Business Continuity



Confidence in the Connected World

Quick Links:

[CIS Controls](#)

[CIS Benchmarks](#)

[CIS](#)

Cybersecurity Best Practices

Cybersecurity Tools

Cybersecurity Threats



Home • Resources • Whitepapers • Internet of Things Security Companion to the CIS Controls

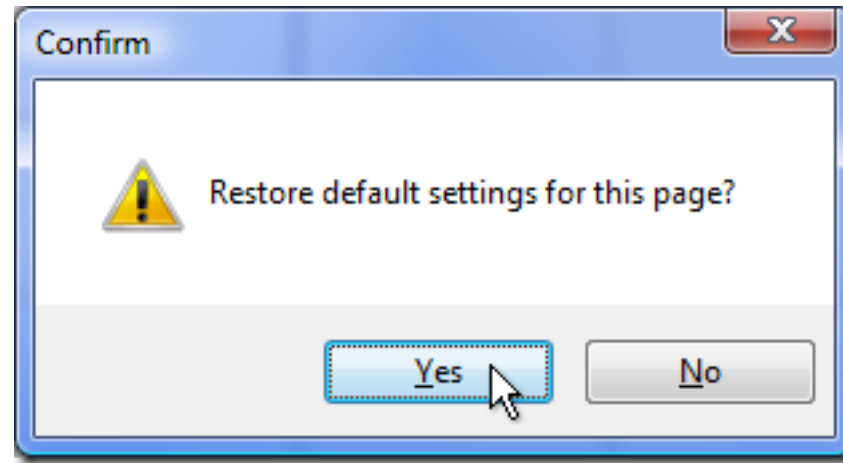
Internet of Things Security Companion to the CIS Controls

Learn how the CIS Controls are applicable to IoT.



IoT – What else can be done?

Protect Revenue, Assist Governance and Ensure Business Continuity



Bitdefender BOX



UPDATE



Questions?



Thank you!

Anthony English

CISSP, CIPP/C, ISO27001 Master, CISM, CISA, CGEIT,
ISO27033 Lead Cybersecurity Manager, MCSE, CRISC, HiTrust Certified Practitioner

mariner
SECURITY SOLUTIONS

The logo for Mariner Security Solutions features the word "mariner" in a bold, lowercase, sans-serif font, with the "a" and "i" having a unique, rounded shape. Below it, the words "SECURITY SOLUTIONS" are written in a smaller, all-caps, bold, sans-serif font. To the right of the text is a stylized network icon consisting of a vertical line with several horizontal lines branching out to the right, each ending in a small circle, resembling a network node or a stylized letter "K".