Presentation overview

• Overview of Eaton
• The threats
• Eaton cybersecurity strategy
• Partnership and collaboration
Eaton overview

We make what matters work.*
Solving industry’s toughest power management challenges around the world.
## Electrical Sector
- 2017 Sales: $12.9 B
- Electrical Products
- Electrical Systems & Services

## Industrial Sector
- 2017 Sales: $7.5 B
- Aerospace
- Hydraulics
- Filtration
- Vehicle

### Financial Summary
- **Total sales**: $20.4 Billion USD
- **Net income**: $3.0 Billion USD

### Key Information
- **Headquarters**: Dublin, Ireland
- **Chairman & CEO**: Craig Arnold
- **Key locations**: Cleveland, United States; Shanghai, China; Morges, Switzerland; São Paulo, Brazil
- **Regional engineering teams** to support products and custom solutions
- **Customers in more than 175 countries**
- **Approximately 96,000 employees**
Power management systems are much more complex
The threat?

BlueBorne: Bluetooth bug could expose billions of devices to attack, cyber experts warn

Internet security experts are urging people to update their software to protect against a serious vulnerability, which, if exploited, could spread uncontrollably via the common wireless technology Bluetooth.

The so-called "BlueBorne vulnerability" could allow hackers to spread from device to device over Bluetooth without the user realizing it.

Ty Miller, managing director of international cyber-security firm Threat Intelligence, said that could be one of the most dangerous security flaws that has come out this year.

Researchers discovered a critical remote code execution vulnerability in two Schneider Electric industrial control-related products that could give attackers the ability to disrupt or shut down plant operations.
Eaton’s approach to cybersecurity

“Driving security in our solutions through training, process, technology, best practices and industry standards”

Our Customers
We deliver high-quality, secure products and innovative cybersecurity services and solutions that reduce risks to our customers.

Secure Product Development
We are passionate to help development teams build solutions that are smart and secure. We do this by integrating ‘Security by Design’ philosophy throughout the lifecycle of a solution.

Expertise Areas
We provide security expertise to embedded systems, power and energy management systems, web and mobile applications, wireless technologies, cloud solutions and IoT systems.

Governance, Regulations, Standards and Partnerships
We learn and bring outside-in perspective to drive tomorrow’s cybersecurity requirements into our solutions today and provide our lessons learnt to standard bodies to help improve the industry requirements.

Incident Response
We are agile and ensure swift vulnerability remediation and incident response to protect Eaton’s brand and business.

Eaton product cybersecurity center of excellence
Secure by design
# Product cybersecurity CoE - Focus and Scope

## Focus areas
- Secure Life Cycle Development
- Governance, Regulations and Standards
- Building internal capabilities through training
- Partnership with leading institutions and companies

## Technology expertise
- Industrial Control Systems
- Distributed Energy (and Microgrid)
- Web and Mobile Applications
- Wireless Technologies
- Cloud Applications
- IIOT

## Technical competencies

---

In scope: Products with intelligence/embedded logic irrespective of external connectivity
Eaton «Secure by Design» approach

Cybersecurity requirements are integral part of the product requirements
Eaton cybersecurity framework for Products

Eaton cybersecurity framework for Products

Product Development Lifecycle

- Incidence Response Analysis
- Design
- Implement
- Verify/Assessment
- Release
- Requirements

Inherent to all phases

Products

- Power Xpert Energy Optimizer
- Power Xpert Solar
- Power Xpert Meter
- LV Switchgear
- Energy Power Management Software
- Molded Case Circuit Breaker
- Eaton Home Automation Hub

© 2018 Eaton. All Rights Reserved. <ETIPP IP Level 1: Eaton Confidential>
Eaton cybersecurity framework for solutions

- Scalable, Adaptable, and Flexible security architecture

- Defense in Depth Strategy
  - Multiple layers of defenses to mitigate security risk
  - Architectural zones, segmentation, and enclaves
  - Isolate DCS Networks with firewalls, routers, IDS
  - Personnel, Policies, Technology, Process
  - Static nature of a ICS lends itself to this strategy
Eaton cybersecurity framework for engineering services

- Trend Micro OfficeScan (real time scan on access and weekly full drive scans + pattern updates pushed to clients as soon and released by vendor)
  - AntiVirus
  - AntiSpyware
  - Web Reputation Service
- Trend Micro Vulnerability Protection (pattern & rule updates pushed to clients as soon as its released by vendor, rules are deployed based on agent’s inventory of software installed on PC)
  - Host Intrusion Prevention Service
  - Virtual Patching
- PhishMe
  - PhishMe Reporter Outlook plug-in
  - Monthly phishing awareness campaigns
- Bomgar (Avecto) DefendPoint - Privilege Escalation Manager
- Check Point Endpoint Security
  - Firewall
  - Application Blacklisting
- CrowdStrike – Endpoint Detection and Response
- CyberArk - Local System Administrator management
- Microsoft
  - Windows Bitlocker full disk encryption
  - System Center Configuration Manager (SCCM) monthly patch cycle + 72 hour deployment for out of cycle critical patches
- PulseSecure (formerly Juniper) - SSL VPN Client – split tunneling disabled while remotely connected to Eaton
Eaton products cybersecurity maintenance lifecycle
Eaton - first certified lab under UL2900 standard

- Positions Eaton as a “first mover” in cybersecurity for our product space
- Help establish a measurable cybersecurity standard for our market segments
- Demonstrate our investment and commitment in cybersecurity
- Provide elements of trust and support to our customers
- Level of assurance for Eaton from our suppliers
Building capabilities through external partnerships
Eaton cybersecurity – monitoring and reporting

Eaton.com/cybersecurity

Central resource for cybersecurity news, solutions, documentation and support
Contact us with questions

Max Wandera, CISSP, GSLC
Director of Product Cybersecurity
Center of Excellence
MaxBWandera@eaton.com