Cybersecurity Essentials: Toolkit for Small Businesses

written by Lauri Moon | November 27, 2023

Dive into the critical digital tools that form the cybersecurity backbone for small enterprises. This session demystifies the technical jargon and focuses on practical, accessible solutions that provide robust protection without complexity.

Register

The Evolving Business of Malware – How to Keep Your Manufacturing Business Running During the Next Outbreak

written by Lauri Moon | November 27, 2023

Join Revolutionary Security cyber experts to learn how ransomware is evolving, and what it means to your manufacturing business. We'll review 2019 ransomware attacks, top lessons learned by the industry and what the next outbreak could look like. Using actual examples of malware incidents our team responded to, you'll learn

just how sophisticated and revenue-focused the attackers behind recent ransomware campaigns are. Leave with recommendations you can immediately put into practice to protect your environment. This presentation is certain to be eye-opening, engaging and helpful in your efforts to ward off cyberattacks.

Attendees will learn:

- New trends in malware targeting manufacturing
- Valuable attack findings from our 2019 incident response team
- Actionable best practices to protect production

Speaker

Jon Taylor, Research and Development Lead Principal, Revolutionary Security

Jon is the Principal Lead for Revolutionary Security's Operational Technology (OT) Research and Development area. While with Revolutionary Security, Jon has led R&D efforts with multiple National Labs and utility clients, pushing forward security technology in OT applications and environments. He is also responsible for Industrial IoT and ICS hardware security research within Revolutionary Security. Jon has recently served as a Senior Manager for the OT practice, where he led long term engineering and design programs, as well as traditional assessment and penetration testing projects in the OT space.

Jon specializes in OT/ICS/IoT security architecture, ICS/IoT device security, secure engineering principles and design, and secure development life cycle (SDLC) for ICS / IoT engineering groups. Jon has also been recognized for his technical depth in product security and communications security, as well as his leadership capability to drive production solutions to completion.

Prior to joining Revolutionary Security, Jon accumulated over 15 years in applied ICS/OT/IoT ecosystem security and engineering experience. Most recently, Jon was a

security architect for Caterpillar's autonomous machines programs and also previously served as a systems engineer in their Information Products division, which focused on vehicle telematics, real-time data acquisition, and remote connectivity. In this role, he was responsible for existing product security evaluation and remediation efforts, as well as planning and executing engineering security improvement plans for world-wide development teams. Jon also served CISO for an embedded technology manufacturer, and had responsibility for existing and generational product security development across all product lines, as well as product and service integration with customer security frameworks. In this role, Jon led the external business interface for security-related items, as well as all internal security processes and development.

Jon holds multiple active security certifications, including CISSP, GICSP, and GRID. He also speaks regularly at security events including SANS ICS Summits, Digital Bond S4, DistribuTECH, and ARC Forums, and is an active member of the SANS Advisory Board. Jon received his bachelor's degree in electrical engineering from Bradley University.

Register

Building a Culture of Cybersecurity Awareness for Employees in Manufacturing

written by Lauri Moon | November 27, 2023

Even the best information technology infrastructure won't stop a well-meaning employee from clicking a malicious link or providing their password over the phone to someone impersonating your IT department. Cyber criminals know that manufacturing companies invest in this infrastructure, so employees are both the weakest link and best entry point to access the companies crown jewels. Building a culture of awareness within the organization teaches employees to identify and mitigate cyber risks. In this webinar you'll learn how to develop a culture of cybersecurity awareness in your organization, train employees to identify cyber risks, and reduce this risk of security breaches.

Register

DoD Cybersecurity Compliance Training Video

written by Lauri Moon | November 27, 2023

Are you a Department of Defense contractor? This video, created by our sister center in Georgia, provides a step-by-step guide on how government contractors can achieve compliance with the new cybersecurity requirements established by the U.S. Department of Defense.

Not sure if you're in compliance? Contact IMC, we can help.

Webinar: Building Resilience Against Cyber Shocks

written by Lauri Moon | November 27, 2023

The smart factory is at the heart of Industry 4.0. Here, advanced software enables machines to communicate and make decisions, while artificial intelligence, robotics, and 3-D printing transform the way products are made and people perform work. But Industry 4.0 also creates new risks and requires manufacturers to integrate security and privacy safeguards into their businesses and throughout their ecosystem — from suppliers to customers. Without these safeguards, manufacturers are vulnerable to cyber shocks — that is, large-scale events with cascading disruptive consequences — has never been more important.

Many manufacturing companies in PwC's 2018 Global State of Information Security Survey say that despite an awareness of disruptive cyber risks, they remain unprepared to deal with them. This suggests that even though manufacturers are thinking more strategically about cyber risk management, they stand on purely defensive footing against cyber risks and are just beginning to adopt leading practices and technologies to fight cyber risk.

Industrial Manufacturers know they need a significant and sustained uplift of talent and technology to fight cyber risk. A sophisticated adversary can too easily target many Industrial Manufacturing companies.

This webinar explores where industrial manufacturers are most vulnerable to cyber disruptions – and how organizations can build integrated safeguards to sustain operations and avoid the common pitfalls.

Speaker

- **E. Quentin Orr, Consulting Partner, PwC**

PwC consulting partner, E. Quentin Orr, or Q, has 20 years of business experience focused on consulting with companies on information security and governance. He has extensive experience in the Industrial Products. Q works with clients to take a business focused approach to cyber security, by guiding their strategy to focus on the most critical information that represents a competitive advantage and drives top and bottom line revenue. He then helps clients develop tailored, economically feasible approaches to maximize the efficiency of their scarce security resources.

Technical Details

This webinar will be conducted using a slides-and-audio format. After you complete your registration, you will receive a confirmation email with details for joining the webinar.

Register