Manufacturing Sector

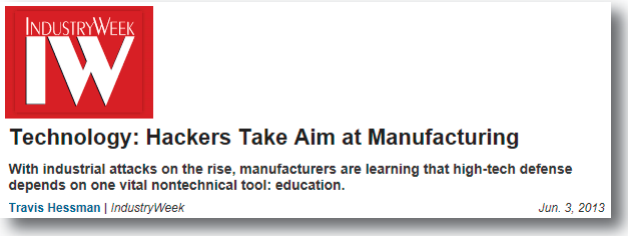
Cybersecurity Workshop

Security is not something to take for granted.

- Internal Threats
- Terrorists
- Industrial Espionage
- Organized Crime
- Hactivists & Hackers

Manufacturers balance safety, quality, standards and compliance with regulations as part of everyday operations. Cybersecurity, with threats from a variety of external and internal sources, is a growing area of concern with both direct and indirect impacts that can target practically any aspect of the organization.

In light of the growing cyber threats to critical infrastructure and the overall national economy, the Administration has proposed incentives for Manufacturers in the form of tax breaks, grant programs, and other efforts recognizing the criticality to the economy manufacturing plays.


INDUSTRYWEEK IW

Technology: Hackers Take Aim at Manufacturing

With industrial attacks on the rise, manufacturers are learning that high-tech defense depends on one vital nontechnical tool: education.

Travis Hessman | *IndustryWeek* Jun. 3, 2013


THE WALL STREET JOURNAL. ≡ U.S.

JOURNAL REPORTS: LEADERSHIP

Departing Employees Are Security Horror

Many think nothing of taking confidential company information with the


CNNMoney
A Service of CNN, Fortune & Money

STATE OF SMALL BUSINESS

Cyberattacks devastated my business!

CNNMoney

From a small startup that was hacked by Anonymous to a cleaning firm that fell prey to a Nigerian scam, these five small businesses explain how cyberattacks hurt their firms.


Los Angeles Times

General warns of dramatic increase in cyber-attacks on U.S. firms

July 27, 2012 | By Ken Dilanian | Los Angeles Times Staff Writer

Who Should Attend?

This workshop is an interactive session designed to take manufacturing executives and managers through an exercise to assess their own organizations and develop pragmatic action plans to implement with their teams.

Executive Order 13636 – Improving Critical Infrastructure Cybersecurity directs NIST to develop a framework that can be adopted across industries to improve enterprise wide security posture. The framework is being developed to help private businesses address the growing risk around cyber threats and impacts to the nation's economy and security.

Northcross Group (NCG) is part of the NIST working group developing the Critical Infrastructure Framework. To the effort, NCG brings experience and lessons learned from manufacturing and other sectors. NCG works with organizations to tailor programs to better understand and improve their security posture. With an approach that security be part of the overall operations and not an impediment, NCG has successfully integrated cybersecurity into existing initiatives as well as implemented new capabilities and functions where needed.

For more workshop information, please contact NCG at:
workshops@northcrossgroup.com
or 207.699.5540

Workshop Objectives

Participants in the workshop will gain a general understanding of how cybersecurity factors into the different components of the manufacturing enterprise.

1. **How to get your arms around security for the entire enterprise.**

2. **The basics of Cybersecurity Preparedness:**
   a. Know what is important and keeping tabs on changes in the enterprise
   b. Protecting important data and systems
   c. Detecting security issues
   d. Responding to an incident
   e. Recovering from an incident
   f. Complying with regulations, standards, and other requirements

3. **Manufacturing Realities – how cybersecurity considerations fit into key quality, logistics, operations, safety, and control systems unique to manufacturing.**
   a. Interconnected business networks
   b. SCADA and Control Systems
   c. Programmable Logic Controller (PLC) controls
   d. Safety Instrumented System (SLS) controls

4. **Tools to implement and structure to manage security in a sustainable and adaptable fashion.**

5. **Key Pitfalls:**
   a. Complexity and cost
   b. Applicability to different parts of the organization
   c. Lack of responsibility and accountability
   d. Lack of applicability

6. **Assessment Exercises – work through templates that can be taken back to the organization as starting points to build or enhance security capabilities.**

7. **Building Your Roadmap – after the workshop, what are 5 key things that you can start the very next day to start improving security across your enterprise.**

NORTHCROSS GROUP

The Northcross Group (NCG) helps organizations understand how technology, people, and security relate in their organization. NCG tailors programs and enhancement to meet business goals, gain competitive advantage, enhance security, implement governance, ensure compliance, and stabilize operations.

NCG consultants bring a blend of technical and business acumen with a proven track record in the public, private, and non-profit sectors. NCG uses disciplined processes, refined from decades of experience. Flexibility is a cornerstone of our industry-tested methodologies—giving NCG the ability to adapt to changing environments and needs.

www.northcrossgroup.com
info@northcrossgroup.com

100 Middle Street, East Tower, #203
Portland, ME 04101
Phone 207.699.5540
Fax 207.699.2113

1101 Wilson Boulevard, 6th Floor
Arlington, VA 22209
Phone 703.351.3397
Fax 703.351.5298