Cyber (In)security
Elements of a Cybersecurity Information Security Plan: How and Why You Need One

Presented by:
Roy Luebke - GENEDGE Innovation and Growth Consultant
Carter Schoenberg, HEMISPHERE Cyber
September 27, 2017
What is GENEDGE?

We are the Manufacturing Extension Program of Virginia

An Economic Development unit of the Commonwealth of Virginia

Part of the Department of Commerce / NIST network of Centers across the country (60 centers, 1500 staff nationally)

20 years of success supporting Virginia businesses

Since 2000, the #1 Bottom-Line and Top-Line Impact Producer in the system - over $3.5 Billion of business impact reported

Over 10,500 industrial jobs created / retained

32 staff including two sub-recipient partners, The Manufacturing Technology Center in SW VA and Old Dominion University in Hampton Roads
What Does GENEDGE Do?

- Strategic Innovation and Growth
- Continuous Process Improvement
- Sustainability
- Supply Chain Optimization
- Technology Acceleration
- Export Assistance
- Market Commercialization
Security is a Combination of Things

- Policies
- Technology
- Behaviors (social media, email)

9/27/2017
Information Security Planning

It’s NOT an exercise in SHELFWARE

DILBERT, I WANT YOU TO AUDIT THE SOFTWARE WE HAVE ON OUR SYSTEMS.

WHY?

SO WE KNOW WHAT WE HAVE.

WHO WILL USE THE INFORMATION?

IT’S JUST IMPORTANT TO HAVE.

IT WILL BE OUT OF DATE BEFORE I’M EVEN DONE.

DO YOUR BEST.

THE BEST WAY TO COMPILE INACCURATE INFORMATION THAT NO ONE WANTS IS TO MAKE IT UP.

I HOPE NO ONE EVER COMES HERE TO LEARN OUR BEST PRACTICES.

9/27/2017
What Is An Information Security Plan?

Focus: Improve protection of information system resources

Goal: Reduce the overall risk of loss when a breach occurs...which WILL happen (ask Equifax’s ex-CEO)

Plan: Ranges from cyber attack prevention through business recovery

Why: The process of documenting will expose gaps
What Is An Information Security Plan?

Documentation of the *structured process* of planning adequate, cost-effective security protection for a system

Input from various managers with *responsibilities* concerning the system, including information owners, the system owner, and key stakeholders

May require *industry-specific requirements*, reporting, auditing
  - Department of Defense DFARS 7012
  - NIST SP 800-171 specifications
Carter Schoenberg - President

www.hemisphercyber.com
Downloadable Self-Assessment

http://www.genedge.org/cybersecurity-assessment-request
Summary of Support:

• GENEDGE services can help identify your weak spots, decrease the costs of increasing your security

• We work with technical firms to conduct a vulnerability assessment

• Provide you with a gap analysis

• Work with you to prioritize the gaps and target spending to protect “Crown Jewels”

• Help develop an implementation plan to close the gaps

• Provide guidance on completing an Information Security Plan
Thank You For Attending

GENEDGE

To Help Improve Your Security Posture

And Reduce Cyber Risks

Roy Luebke
Email: rluebke@genedge.org
Cell: 276-732-8372