Cyber (In)Security
What Business Leaders Need To Know

Presented by:
Roy Luebke
Innovation and Growth Consultant

July 12, 2017
What is GENEDGE?

We are the Manufacturing Extension Program of Virginia

A 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

Growth
First Thing To Know.....

YOU HAVE ALREADY BEEN COMPROMISED
First Thing To Know.....

There is no such thing as cyber security

...... only more secure or less secure

...... the degree is a matter of money and priorities

- A New Zero-Day Vulnerability Discovered Each Week
- Half a Billion Personal Records Stolen or Lost
- Spear-Phishing Campaigns Targeting Employees Increased 55 Percent
- Ransomware Increased 35 Percent
- 100 Million Fake Technical Support Scams Blocked
- 430 million new unique pieces of malware in 2015, up 36 percent from the year before
- Major Security Vulnerabilities in Three Quarters of Popular Websites Put Us All at Risk
- New Mobile vulnerabilities increased 214%
Why Small Businesses?

- In 2015, 43 percent of all Spear-Phishing attacks targeted businesses with fewer than 250 employees*

* Symantec 2016 Threat Report
Risks in Cyber

Indiscriminate Attacks

Destructive Attacks

Cyber Warfare

Espionage: Both Corporate and Government

Email and login

Financial and personal information

Medical information

Hackivism
Types of Cyber Issues - Technical

- **Vulnerability of a system**
  - Eavesdropping
  - Spyware
  - Phishing
  - Espionage

- **Exploits to/within a system**
  - Trojans
  - Virus and worms
  - Denial of service
  - Botnets
  - Adware
  - Dialers
  - Ransomware

- **Payloads delivered onto a system**
  - Rootkits
  - Keyloggers
Vulnerability:
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source
Types of Threat Vectors

- Spoofing
- Snooping
- Social engineering
- Increasing the level of system privileges
- Ransomware
Types of Threat Vectors

• **Identity Theft** - steal & misuse your identity ($$$)

• **Phishing** - Email tricking YOU or your employees into giving personal or business/customer information (a form of social engineering)

• **Spear Phishing** - Email with specific company details and targeted at specific employees to deceive you/the target into responding

• **SPAM** - Unsolicited and unwanted Email

• **Compromised web pages** - invisible code planted on legitimate web pages which will attempt to install malware on your personal or business computer(s)
Who Is Behind That Computer?
Seriously Bad Guys

China
PLA Unit 61398

Military Unit Cover Designator (MUCD) of a People's Liberation Army advanced persistent threat unit that has been alleged to be a source of Chinese computer hacking attacks.

Russia
FSB/KGB

the Russian signals intelligence, which is currently a part of the FSB but has been formerly a part of 16th KGB department, but others are directed by the Russian Ministry of Internal Affairs and the Military of Russia.
North Korea In On It Now?

- WannaCry Ransomware Attack
- Hit 100 Countries
- Uses code stolen from NSA via Wikileaks
- Microsoft emergency patch to Windows XP
- One happy accident stopped it in USA
- Would not be affected if users had updated security patches from Microsoft available back in March!

WHAT WOULD YOUR COMPANY DO IF ATTACKED?
Malicious Attacks - What are they after?

- Access to business information / money
- Personally Identifiable Information (PII)
  - Your own
  - Your employees'
  - Your customers'
- To use your personal or business resources for their own purposes / activities
- Disrupt business operations
They Want Your Supply Chain

Customers

Suppliers

Distribution

Internal Enterprise
What is Information Security?

- Personnel Security
- Operational Security
- Contingency Planning & Disaster Recovery
- Physical Security
- Privacy
- Cyber-security
What is Information Security?

Confidentiality
Unauthorized Access, Disclosure

Integrity
Unauthorized Modification, Use

Availability
Disruption, Destruction
What Is Cyber “Security”?  

Prevention ---- Where the $ have been in past  

Detection ---- Where the $ are moving to now  

Responses ---- Taking action during the attack  

Recovery ---- Fixing the damages of an attack
Manufacturing Threats

- Intellectual property
- Manufacturing lines (PLCs designed in the 80s)
- Chips coming on suppliers’ products
- Viruses going out on your equipment into the supply chain
- *Small companies are the weakest link and therefore key targets of nefarious actors*
What Is Coming in Cyber World?

Internet of Things:
- Cars
- Smart home devices
- Medical devices
- Smart TV’s
- Embedded devices

Gartner: 6 billion things connected by 2016
21 billion things by 2020
What Happens When You’re Hit?

Most Small Businesses Don’t Recover

- 20% of all cyber-attacks hit small businesses with 250 or fewer employees
- Nearly 60% of small businesses go out of business within 6 months after being victimized by cybercrime.

Small businesses face greater threat from computer hackers

- Small businesses are increasingly being targeted because their security is not as tough.
More Money Spent on Regulations

U.S. Mid-Atlantic manufacturers on average have devoted more money to complying with regulations than to security on either their data and networks, or equipment and workers, a Philadelphia Federal Reserve 2016 survey showed.
DFARS for Defense Contractors

- Defense Federal Acquisition Regulation Supplement (DFARS) and Procedures, Guidance, and Information (PGI)

- Safeguarding covered defense information and cyber incident reporting

- **Must be compliant by 12/31/2017 !!!**
Dept. Defense Cyber Compliance

- **FAR 52.204-21** (15 Basic Security Controls)

- **DFARS 225.204-7012** (110 Security Controls)
  - Includes the NIST SP 800-171 specs
NIST SP 800-171

Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

- Prime contractors AND
- Subcontractors
For Small Business CEOs

Virus protection

Firewall

Email filter

IS NOT GOING TO PROTECT YOUR ASS
Who’s Problem Is It?

It is not an IT problem.....

It is a LEADERSHIP risk management issue
What Is The Solution?

CYBER RISK Management
You Are Already Compromised!

Your systems and infrastructure are already breached, you just have not found out yet.

Significant risk exposure to loss of intellectual property, customer and staff information, and connections to partners through breaches to IT infrastructure, communications, and automated systems.

Risk exposure in manufacturing production by having cyber threats unintentionally installed on products via chips, or any internet connectivity to or through products.

Loss of IT infrastructure, or having cyber threats placed onto their offerings, could put many firms completely out of business.
Small Businesses Are Targets

Travelers Insurance reports that 62% of cyber breach victims are small to medium businesses.

Healthcare and Financial are most-breached industries currently

Cyber Breach Cost Components

Business income loss
Defense and settlement costs
Lost customers and damaged reputation
Cyber extortion payments
Forensics costs to discover cause
Regulatory fines
Cost to notify regulators
Cost to notify affected individuals and companies
Cost to rebuild infrastructure, data, etc.
Loss of intellectual property
Loss of other assets
Mitigate With Cyber Insurance

- Risk management mechanism
- Costs of response/recovery
- Awareness to make claim

Policy Payout Data
Avg Nano-cap: $56,000
Avg Micro-cap: $150,000

7/12/2017
What is Risk?

The probability and impact of a negative outcome in a given period of time

- Lack of information results in uncertainty
- The amount of potential loss
Mitigate Risk Exposure

- Reduce unexpected business recovery expenses
- Minimize technology losses and expenses
- Minimize financial losses
- Minimize intellectual property losses
- Decrease liability costs due to products being cyber threat hosts
- Avoid spending money on unusable/unneeded tools
- Avoid failure to meet regulatory requirements or government compliance
- Identify where security risks are possible/probable
- Reduce negligence in protecting assets
- Improve executive decision making
- Increase knowledge of cyber law
- Define public relations plan to prepare for an inevitable security breach
- Cyber security needed down to the Internet of Things IoT level
Start With NIST Cyber Framework

- Identify
- Protect
- Detect
- Respond
- Recover

http://www.nist.gov/cyberframework/
# NIST Cyber Framework

<table>
<thead>
<tr>
<th>Function Unique Identifier</th>
<th>Function</th>
<th>Category Unique Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identify</td>
<td>ID.AM</td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.BE</td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.GV</td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RM</td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td>PR</td>
<td>Protect</td>
<td>PR.AC</td>
<td>Access Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.AT</td>
<td>Awareness and Training</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.DS</td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.IP</td>
<td>Information Protection Processes and Procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.MA</td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.PT</td>
<td>Protective Technology</td>
</tr>
<tr>
<td>DE</td>
<td>Detect</td>
<td>DE.AE</td>
<td>Anomalies and Events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.CM</td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.DP</td>
<td>Detection Processes</td>
</tr>
<tr>
<td>RE</td>
<td>Respond</td>
<td>RS.RP</td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.CO</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.AN</td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.MI</td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td>KU</td>
<td>Recover</td>
<td>RC.RP</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.CO</td>
<td>Communications</td>
</tr>
</tbody>
</table>
Steps To Stronger Cyber Security

1. Prioritize and Scope Assets To Protect
2. Orient
   To related systems and assets, regulatory requirements, and overall risk approach. Then identify threats to, and vulnerabilities of, those systems and assets.
3. Create a current profile
4. Conduct a risk assessment
5. Create a target Profile
6. Determine, analyze and prioritize the gaps
7. Implement action plan
GENEDGE Risk Process

1. Establish the context
2. Conduct Risk Assessment
3. Implement Risk Treatment
4. Communicate and Consult
5. Monitor and review the risks and controls
Risk Mitigation

Cyber disaster planning and recovery – reduce the risk

Supply chain partners – transfer the risk

Security policies and training – avoid the risk

Use Cyber insurance

Consult Cyber attorneys regarding contracts
Things to do

• Train your employees
  – Phishing
  – Social Media

• Clean machines
  – Patches
  – Latest security software
  – Browsers
  – Operating Systems

• Use firewalls
Things to do

Mobile Devices
- Passwords
- Encrypt
- Install Security Apps
- Avoid Public Networks
- Report if lost or stolen
Things to do

- Make backups
  - Automatically
  - Weekly
  - Store offsite or in the cloud

- User Accounts for each employee
  - Strong passwords
  - Admin privileges limited
Things to do

- Secure Your Wi-Fi
  - Encrypt
  - Do not broadcast network name
    - Service Set Identifier (SSID)
  - Password protect router
Things to do

• Payment Cards
  – Trusted and validated tools
  – Anti-fraud services
  – Isolate payment systems

• Limit Access
  – No one has access to all
  – Based on roles
  – SW Install needs permission
Things to do

• Strong Passwords
  – Change every three months
  – At least 12 characters
    • Number
    • Special character
  – Multi-factor Authentication
  – Train Employees
Downloadable Self-Assessment

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

• Cyber (in)Security is a HUGE and GROWING Issue

• If you are playing, you are a target

• Compliance and Regulatory issues uncertain and growing

• 60% of SMBs go out of business following a breach

• There are AFFORDABLE ways to get help
Thank You For Attending

Contact GENEDGE To Improve Your Security Posture And Reduce Cyber Risks

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

7/12/2017