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

Growth
First Thing To Know.....

YOU HAVE ALREADY BEEN COMPROMISED
What Is The Solution?

CYBER RISK

ASSISTANCE!!
First Things First

- **Identify your assets to be protected**
  - Intellectual property
  - Electronic assets
  - Business relationships/supply chain
  - Download self-assessment
    http://www.genedge.org/cybersecurity-assessment-request

- **Conduct an external vulnerability assessment**
  - NOT a penetration test (PEN test)
Sources of Help: Cyber Insurance

- International Risk Management Institute
  
Dark Reading

- From Information Week

Sources of Help - DHS

- U.S. Department of Homeland Security
- For critical infrastructure every day to provide energy, water, transportation, financial systems
  https://www.us-cert.gov/ccubedvp

- https://www.dhs.gov/topic/cybersecurity

- DHS Computer Cyber Division
DFARS

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

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

- NIST SP 800-53
  - Security and Privacy Controls for Federal Information Systems and Organizations

- NIST SP 800-171
  - Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
DISA – Defense Information Systems Agency

- Joint information environment

- [http://www.disa.mil/about/our-work/jie](http://www.disa.mil/about/our-work/jie)
  - Cyber security/information assurance program

- [http://dibnet.dod.mil/](http://dibnet.dod.mil/)

- External Certificate Authority Program (for third parties to securely communicate with the DoD and authenticate to DoD Information Systems)
  - [http://iase.disa.mil/pki/eca/Pages/index.aspx](http://iase.disa.mil/pki/eca/Pages/index.aspx)
To file complaints about cyber crime:


- For tips:
  

https://www.fbi.gov/investigate/cyber
Industrial Controls

- Industrial Controls Cyber Security
- The National Cybersecurity and Integration Center (NCCIC), a division of the Department of Homeland Security's Office of Cybersecurity and Communications (DHS CS&C)

- https://ics-cert.us-cert.gov/About-Industrial-Control-Systems-Cyber-Emergency-Response-Team


- https://scadahacker.com/library/
Industrial Controls
MACH37™ is America’s premier market-centric cybersecurity accelerator.

The Accelerator is designed to facilitate the creation of the next generation of cybersecurity product companies. MACH37's unique program design places heavy emphasis on the validation of product ideas and the development of relationships that produce an initial customer base and investment capital.

MACH37 is located at the Center for Innovative Technology. The Accelerator is operated by the MACH37 partners.

- https://www.mach37.com/
Sources of Help - NIST

- U.S. Department of Commerce – National Institute of Technology
  - https://www.nist.gov/topics/cybersecurity

- NIST Cyber Framework: https://www.nist.gov/cyberframework

- NIST National Cybersecurity Center of Excellence
  - https://nccoe.nist.gov/
NIST/DHS Vulnerability Database


Vulnerability Search Engine
National Checklist Program
SCAP Validated Tools
Visualizations
CVSS V3 Calculator
Data Feeds
Product Dictionary
Vulnerability Metrics
Vulnerability Categories
CVSS V2 Calculator
The SANS Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. A range of individuals from auditors and network administrators, to chief information security officers are sharing the lessons they learn and are jointly finding solutions to the challenges they face.

https://www.sans.org/

- Training and certifications
- Guidance
- Resources: https://www.sans.org/security-resources/
Virginia State Government

- http://cyberva.virginia.gov/
- https://virginiacyberrange.org/
- http://cyberva.virginia.gov/resources/?iama=Professional
- http://cyberva.virginia.gov/resources/
Universities

- Virginia:
  For a listing of all education and support programs available: http://cyberva.virginia.gov/colleges/

- University of Maryland:
  https://cyberchain.rhsmith.umd.edu/

- Norfolk State University/Old Dominion University:
  https://www.nsu.edu/cset/csetgraduate/cybersecurity/index
Key Commercial Sites

- Kaspersky labs  https://usa.kaspersky.com/
- FireEye  https://www.fireeye.com/
- Symantec  https://www.symantec.com/security_response/
- McAfee  https://community.mcafee.com/community/home
- IBM  https://www.ibm.com/security/
The “Bigger” Options

- **On-Premise Managed Services**
  - Old PCs? Old printers? Old software?

- **Cloud based**
  - Entire systems
  - Platforms as a Service (PAAS)
  - Software as a Service (SAAS)
  - Data sharing services/content
  - Specific applications
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
# Cyber Firms in Virginia

<table>
<thead>
<tr>
<th>Company</th>
<th>Website</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Lion</td>
<td><a href="http://redlion.io">http://redlion.io</a></td>
</tr>
<tr>
<td>Hemisphere Cyber Risk Management</td>
<td><a href="https://www.hemisherecyber.com/">https://www.hemisherecyber.com/</a></td>
</tr>
<tr>
<td>Talatek</td>
<td><a href="https://talatek.com/">https://talatek.com/</a></td>
</tr>
<tr>
<td>Tiber Creek Consulting</td>
<td><a href="https://tibercreek.com/">https://tibercreek.com/</a></td>
</tr>
<tr>
<td>McClean Insurance (cyber policies)</td>
<td><a href="http://www.mcleaninsurance.com/">http://www.mcleaninsurance.com/</a></td>
</tr>
</tbody>
</table>
List of Virginia Cyber Firms

- The Cybersecurity 500 List

http://cybersecurityventures.com/cybersecurity-500-list/#home/?view_1_per_page=500&view_1_page=1&view_1_sort=field_1|asc&view_1_search=virginia
Summary:

- 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

Contact GENEDGE

To Help Improve Your Security Posture

And Reduce Cyber Risks

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

7/26/17