Cyber Attacks Can be Devastating to Small Manufacturers

The risks are enormous and potentially devastating! 55% of small and mid-sized businesses have experienced a data breach or cyberattack. 43% of spear-phishing attacks are targeted at small businesses. 60% of impacted businesses are left severely impacted.

As a result of increased concerns about cyber-attacks, manufacturers with contracts from the Department of Defense (DoD), General Services Administration (GSA) or NASA must be compliant with defined cybersecurity requirements to protect Controlled Unclassified Information per NIST SP 800-171 or risk losing contracts. Small manufacturers in other supply chains such as automotive, medical, and energy can also expect cybersecurity contract requirements.

Companies should not wait for customer-imposed requirements to identify IT security vulnerabilities and protect their businesses. All manufacturers should take positive steps now to implement and maintain appropriate IT security controls, and know what to do if a breach does occur.

VMEC can provide resources and assistance to help manufacturers take action to protect their business.

These include:
- NIST cybersecurity documents for self-assessment and developing an IT security plan.
- Access to NIST Manufacturing Extension Partnership and MEP National Network cybersecurity experts.
- Professional Services for Assessment, remediation, and security monitoring with local and national cybersecurity experts and service providers.
- Connection to State of Vermont partner resources such as the Vermont PTAC (Procurement Technical Assistance Center) and the VT Attorney General CAP (Consumer Assistance Program) and Small Business Initiative.

VMEC is offering IT Security Services with local IT service provider, rbTechnologies

rbTechnologies is a central Vermont based IT service company operating since 1997. Dave Porcello joined rbTech in 2017 to provide IT security services. Dave is the founder of Vermont security firm Pwnie Express and inventor of the award-winning Pwn Plug security testing device, featured on Good Morning America, NPR, CNN, Forbes, Wired, "Mr. Robot", and winner of SC Magazine’s Innovator of the Year. In his 16 years of field experience, Dave has served as Director of Security for Vermont Mutual, adjunct professor at Norwich University, security counsel for NPR and advisor for public figures including Steve Wozniak and Will Smith.

VMEC and rbTechnologies are offering Vermont manufacturers, including defense contractors, the following services:
- Quick IT Security Assessment (4-6 hours) including walk-through and discussion of SP 800-171 requirements
- Full IT Security Assessment that identifies and documents gaps and vulnerabilities, and a remediation plan outline
- Customized remediation projects
- Continuous proactive security monitoring and assessment follow-ups

Interested in learning more about IT security services? Schedule a no-cost consultation with VMEC today!

Jon Bates, jbates@vmec.org, (802) 345-2062 - Patricia Giavara, pgiavara@vmec.org, (802) 279-6103
Cybersecurity strengthens U.S. Manufacturers

Cybersecurity protects the confidentiality, integrity and availability of your information. A cybersecurity program provides advantages for small and mid-sized manufacturers:

- Improve Recovery Times After Disruptions
- Avoid Potential Losses
- Protect Valuable Data
- Ensure Employee and Customer Privacy
- Mitigate Risks

Reality of Cyberattacks and Breaches

- 55% of small and mid-sized business have experienced a data breach or cyberattack.
- 43% of all spear-phishing attacks are targeted at small businesses.
- 60% of impacted businesses are left severely impaired.
- $38K is the average cost for a small business to overcome a data breach.

Common Types of Attacks and Breaches

- Spear Phishing
- Identity Theft
- Web Attacks
- Ransomware
- SPAM

5 Steps to Reduce Cyber Risks

Protecting the information of your company, employees, and customers is an ongoing process. Manufacturers will benefit from a program that:

- Identifies your assets
- Protects your data
- Detects incidents
- Responds with a plan
- Recovers normal operations

Defense Suppliers: Compliance

Manufacturers in the DoD supply chain have until December 31, 2017 to be in compliance with new DFAR cybersecurity requirements.

Learn more at nist.gov/mep/cybersecurity

Enhance Your Cybersecurity

Whether you’re a manufacturer implementing a cybersecurity program, or a DoD supplier looking to achieve compliance, the MEP National Network can help you with your cybersecurity needs.

Contact your local MEP Center or learn more at nist.gov/mep/cybersecurity


INFOGRAPHIC DESIGNED BY: 24/7 Creative, A Division of Gold Group

www.nist.gov/mep 1-800-MEP-4MFG

National Institute of Standards and Technology
U.S. Department of Commerce