SELF ASSESSMENT FOR YOUR BUSINESSES CYBER POSTURE

Find out how vulnerable your business is.

Taking Inventory :

- ☐ Have you conducted a physical inventory of company owned hardware to ensure all the components, and physical materials are accounted for?
- ☐ Does your business follow any rules for adding hardware to the network, so that it is properly configured before connecting?
- ☐ Do you regularly update a list of all connected devices and use that list to regularly validate that connected devices are approved?
- ☐ Is the software for the devices on your network up to date? This includes all computers, cell phones, printers, access points, & routers.

Data Access & Security :

- ☐ Are all passwords complex and lengthy? (No less than 10 characters, letters upper and lower case, numbers and special characters.)
- ☐ Is all sensitive information encrypted?
- ☐ Is antivirus software installed and constantly updated on your hardware?
- ☐ Are your users required to use Multi-factor Authentication prior to system access?
- ☐ Do you have system backups that are stored offline and offsite?

Securing your Environment:

- ☐ Do you require employees and system users to sign an Acceptable Use Policy, signifying that they understand there is no expectation of privacy when using company equipment and network, that they are subject to monitoring and discipline for violating these policies?
- ☐ Do you establish time periods throughout the year for system checks, for example: to ensure that current users have correct access privileges and that former users have had privileges revoked?
- ☐ Do you have a Bring-Your-Own-Device (BYOD) policy and process for guests and employees that use their personal cell phones, computers, etc. when using company resources?
- ☐ Do you have a system to control physical documents and devices throughout their life cycle?

Access Control:

- ☐ Does your system have role-based access control?
- ☐ Does anyone have universal access? (Even for a one person company.)

Compliance and Training:

- ☐ Does your business need to follow any compliance requirements? (Law, Regulation, Insurance requirements)
- ☐ Do you require your employees to attend a yearly cybersecurity awareness training?

"THIS PROJECT IS FUNDED BY U.S. DEPARTMENT OF DEFENSE, OFFICE OF LOCAL DEFENSE COMMUNITY COOPERATION GRANT THROUGH THE CALIFORNIA GOVERNOR'S OFFICE OF PLANNING AND RESEARCH"

ADDITIONAL RESOURCES

ONE-ON-ONE COUNSELING WITH BUSINESS ADVISOR OR CYBER ADVISOR

SELF ASSESSMENT TOOLS

https://www.utah.gov/beready/business/documents/BRUCyberSecurityChecklist.pdf
www.us-cert.gov-ccubedvp (Self-Assessment Tool)
Fico.com/en/products/cyber-risk-score (Get Your Cyber Risk Score)
https://www.nist.gov/blogs/manufacturing-innovation-blog/how-vulnerable-are-you-cyber-attack-self-assessment-tool (Specific to manufacturing companies)

ONLINE RESOURCES

www.fcc.gov/cyberplanner (Help create a security system plan for your small business.)
https://staysafeonline.org/cybersecure-business/ (Cybersecure my business)
Nist.gov/itl/smallbusinesscyber (Small Business Corner)
Cisa.gov/cyber-essentials (Small Business Toolkit)
https://woodruffsawyer.com/cyber-liability/cyber-101-liability-insurance-2021/ (Article about the basics of cyber insurance.
https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=922797 (Guide for recovery)

"THIS PROJECT IS FUNDED BY U.S. DEPARTMENT OF DEFENSE, OFFICE OF LOCAL DEFENSE COMMUNITY COOPERATION GRANT THROUGH THE CALIFORNIA GOVERNOR'S OFFICE OF PLANNING AND RESEARCH"