C3 VOLUNTARY PROGRAM

Small and Midsize Business (SMB) Leadership Agenda

As the leader of a small or midsize business, you recognize that cybersecurity is critical to any business enterprise, no matter how small. But given the scope and complexity of the issue – in the face of a small staff and limited resources – how do you start a conversation with your leadership team about how to best address your company's needs?

Below are suggested questions and topics you can use to help guide a conversation about your business's current cybersecurity posture and cybersecurity best practices. This agenda can also assist you in starting a conversation about how to use the National Institute of Standards and Technology's (NIST) Cybersecurity Framework as a guide for your cybersecurity procedures and policies.

1. Overview of Cyber Threat

Consider providing a threat briefing to update your team on the current cyber threat environment, especially as it pertains to SMBs.

2. Understanding Risk

Facilitate a discussion about how your company uses information technology (IT) to support your core business culture and functions, how you allocate and support cybersecurity resources, and how you maintain and improve your state of preparedness.

Questions about Our Organization

1) What does our organization value?
2) What are the core business functions or products that our organization provides or produces?
3) What are our most valuable information assets and who might want them?
4) What are the potential confidentiality, availability, or integrity impacts to consumers of our products and services?
5) How does connectivity with our partners, subcontractors, or vendors affect our cyber risk?
6) Do we collect and/or store sensitive personally identifiable information (PII) and/or health data?

Questions about Our Resources

1) Do we have the proper staffing and resources to protect our information and cyber infrastructure? If not,
    a. What resources are we able to allocate toward improving our internal capabilities?
    b. What external services can we access or organizations can we partner with to secure these capabilities?
2) How are decisions made for cybersecurity and resource allocation?
3) How are we informed about industry trends and new technologies?
4) How are risks communicated across the organization?
5) Is our leadership team regularly informed about the level of cyber risks to our organization?

Questions about Our Preparedness

1) What are the biggest challenges our organization faces in managing our cybersecurity?
2) What are the potential health, safety, and environmental risks to our organization if we face a cyber-attack?
3) Do we have robust incident response policies and procedures in place to react swiftly to a cyber-attack? How often are they tested/audited and updated?
4) What are our financial, competitive, reputational, and regulatory risks?
5) With what external organizations do we share our data?
6) Do we have the proper agreements and safeguards in place to protect ourselves?
7) Have we formed partnerships with the Federal government, within our sector, or with cross-sector partners to better coordinate security efforts?

3. Existing Company Security Plans

Discuss the state of existing company security plans with your leadership team.

1) When did we first develop your plans, and when did we last update them?
2) Do our plans address cyber risk management and physical risk management?
3) Who should review the plan(s), both internally and externally?
4) How will we communicate the information in the plan(s) to our employees to ensure compliance?
5) Do our plans address the questions in the sections above?

4. Next Steps for Our Company

Discuss next steps for your company based on your current cybersecurity posture.

1) Which are high priority areas for immediate action?
2) Will we revise our short, medium, and long-term security goals based on our current cybersecurity posture?
3) How often will the leadership team meet to discuss company cybersecurity?

5. Discussion of Government Resources

Discuss which cyber risk management resources would be beneficial to your company.

- **Visit the Critical Infrastructure Cyber Community (C³, pronounced "CCubed") Voluntary Program website** for a list of cybersecurity and risk management tools and resources geared specifically toward SMBs.
    - Locate these resources and more at: www.us-cert.gov/ccubedvp