Cyber Risk Management for Elected Officials

Purpose

Municipal and School Boards play a critical role in cybersecurity preparedness. From understanding organizational risks to making informed decisions about policies, budgets, and resources, board members help shape their community's cybersecurity posture. Our Cybersecurity Training for Public Boards equips members of select boards, town councils, school boards, and other governing bodies with the foundational knowledge needed to ask the right questions, provide effective oversight, and support stronger cybersecurity practices.

Importance of an Incident Response Plan

Every minute counts when a cyber incident strikes. An Incident Response Plan (IRP) gives your organization a tested playbook so staff can respond quickly and confidently:

- **Faster Containment:** Clear steps to detect, isolate, and stop an attack limit damage and shorten downtime.
- **Clear Authority:** Leaders know who decides, who communicates, and who to call.
- **Legal and Regulatory Compliance:** Meets notification rules and preserves evidence.

Boards that require an IRP and support regular tabletop exercises turn a potential crisis into a managed event and protect public trust.

Importance of a Continuity of Operations Plan

A cyber incident can take down email, phones, financial systems, and records for weeks. A Continuity of Operations Plan (COOP) ensures your organization can still provide:

- **Essential Services Without Interruption:** Public safety, utilities, payroll, and education continue during an outage.
- **Clear Roles and Alternate Methods:** Defined succession, backup communications, and manual workarounds.
- **Protection of Vital Records:** Critical data is identified, backed up, and accessible.

Boards that require and fund a COOP reduce downtime, control recovery costs, and preserve public trust when a cyber incident or other hazard strikes.

Importance of Budgeting for Cyber Risk Mitigation

Cyber risk is a budget issue, not just an IT issue.

- **Prevention Costs Less Than Recovery:** Ransomware recovery, legal fees, and lost productivity routinely cost local governments far more than the training, backups, and security tools that could have stopped an attack.
- **Grants Are Not a Long-Term Plan:** Grant programs help organizations get started, but lasting protection requires predictable annual funding for software updates, monitoring, cyber insurance, and staff training.
- **Board Oversight Drives Results:** Regular risk reports and funding tied to measurable goals ensure every dollar reduces real risk.

Call to Action

1. **Develop or Update your Incident Response Plan and Continuity of Operations Plan and exercise them.** The MCDP has free workshops to assist you. To schedule these grant-funded workshops, visit the web link to the right.
2. **Budget for and invest in defining and mitigating the cyber risk to your organization.**



NH Municipal Cyber Defense Program

The New Hampshire Municipal Cyber Defense Program (MCDP), powered by ATOM, is the only sustained program aimed at reducing Cybersecurity risk in New Hampshire Communities. Funded through the NH Department of Information Technology with State and Local Cybersecurity Grant Program funds, it provides Cybersecurity training and workshops to public sector employees and the public at large.

The MCDP mitigates risk in the most vulnerable layers of New Hampshire's Cyber Defense - The Human Intrusion Prevention System, also known as "The User," technical configurations of public sector systems, and insufficient Incident Response Planning and Continuity of Operations Planning. The MCDP builds resilience! MCDP training sessions are tailored to the organization type, individual and team roles, and the organization's existing cybersecurity risk profile.

For more information, please contact:

Ken Weeks
National Security Advisor

Email:
MCDP@theatomgroup.com

Phone:
603.501.0003

Web:
theatomgroup.com/mcdp

New Hampshire DoIT