



The Problem

Cyber threats are on the rise and municipalities are soft targets for criminals. ISSAC is working to help Burlington avoid a cyberattack while also preparing to respond and recover from one should one occur.

Noteworthy cyberattacks from the last three months:

- [Massachusetts Auto Inspections offline for three weeks due to ransomware](#)
- [Criminals increased Sodium Hydroxide levels in water at Florida water plant](#)
- [East Coast Oil Pipeline shutdown due to ransomware attack](#)
- [City of Lawrence hit with ransomware attack in April](#)
- [Schools have become the leading target of ransomware attacks](#)

What is ISSAC doing to help prepare Burlington for a cyberattack

- Met with cyber security analysts from the state
- Developed a Cybersecurity Policy to present to the Town for adoption
- Sent drafts of policy to Town Administrator and ISSAC Select Board representative for their early feedback

Important themes the proposed cyber security proposals

- All Town stakeholders (administration, department heads, employees, vendors, etc.) play a *critical* role in protecting the Town against threats
- Taking important steps *now* prior can help Burlington prevent attacks from happening
- Advanced planning is essential to mitigating an attack and quickly returning to normal operation
- The Town's attack readiness will be improved by periodically rehearsing the Town's attack response and recovery plans

Next Steps

- Present the proposed cybersecurity policy to the Select Board and other supervisory bodies for feedback & adoption
- Once approved, monitor the Town's implementation of the policy
- Recommend changes to the policy as the threat landscape changes

ISSAC Committee Members

Residents

David Hughes
David Miller
Ben Axelrod
Steve Morin
Phillip Pascale

Town

Joe Bongiorno
Robert Cunha
Glenn Mills
Michael Wick

Select Board Rep

Nick Priest

Contributors

Jose DeSousa
Rob Neufeld