Digital Team: Cybersecurity Overview Memo

The digital team would welcome engaging with the transition team and early administration efforts to develop a thorough Cybersecurity strategy. Please find below an overview and directional recommendations to consider.

Major cyberattacks against large commercial enterprises and important Federal agencies have made headlines on a monthly basis over the last several years. Despite garnering less attention, State and local governments also face an increasing cyber threat, in large part because they are often easier to breach than better-defended enterprise networks. The Connecticut government is no exception, and State agencies process and store large amounts of valuable data about individuals, businesses, critical infrastructure, and financial transactions. This combination of high value assets and a less mature defense creates tempting targets for financial crime, disruption of public services, exposure of political figures, or even nation-state sponsored cyber-terror or espionage.

Several recent attacks highlight the potential damage of a cyber-attack on State and local agencies. Although the WannaCry attack that occurred in Connecticut in early 2018 resulted in no data loss, the city of Atlanta was hit by a ransomware attack that stymied some public-facing services, including court systems. The Emotet Trojan attack on Allentown, Pennsylvania's municipal systems disrupted operations of finance and police departments, among others. The Colorado Department of Transportation (CDOT) was hit by a SamSam ransomware attack that forced the shutdown of more than 2,000 endpoints, taking the department back to the age of pen and paper during the investigation and recovery process.

Like most State governments, Connecticut has many older IT systems and operates largely on legacy infrastructure, with a relatively complex network topology. As noted in a recent article on State government cybersecurity: "This type of environment is difficult to manage and secure, creating gaps which attackers readily find and exploit. These issues are compounded by tight budgets, difficulty recruiting security experts, and drawn-out bureaucratic procedures for technology upgrades and purchases. IT and security personnel are typically overburdened and pulled in multiple directions, leading to a reactive security stance that simply isn't sufficient in the face of constant, sophisticated intrusion attempts." Based on initial assessments, this describes CT accurately.

While the previous administration was successful in raising the visibility of Cybersecurity issues, the incoming administration can act to truly advance Connecticut's cybersecurity posture. The current CIO's office has done an admirable job with limited resources, but many gaps remain, and the overall risk level of the

State and municipalities remain unacceptably high. Specifically, based on preliminary document review and conversations with State personnel, the Digital Policy team recommends:

Like Information Technology overall, the Cybersecurity function needs to be elevated, empowered, and more centralized within the State government organization.

- While the current budget environment is challenging, persistent under-investment in Cybersecurity across the government has increased risk and should be remedied as soon as possible.
- It is critical that the state attracts and retains more skilled Cyber and Infosec professionals, both in operational roles and to help drive improvement initiatives. It should also upskill the existing workforce through focused training. Connecticut should invest in an Enterprise Security Operations Center with more complete visibility into network and system events across the government. This SOC should provide 24x7 monitoring and response services.
- Connecticut needs a more integrated approach to identity management, a foundation of modern security architectures. Currently identity systems are fragmented and siloed, which is both more expensive and less effective.
- The state needs to begin moving towards a risk-based “zero-trust” security model as opposed to traditional perimeter security architecture. It should also look to a more automated, integrated security platform as opposed to the traditional collection of poorly integrated (and often mis-configured toolsets).
- Connecticut should develop a strong “Cloud Policy”, which will help IT delivery overall and also leverage the best-of-breed security capabilities of hyper-scale cloud vendors.
- The state should consider investing in supporting regional security offices to help enable struggling municipal Cybersecurity efforts.

Administration officials who are interested in cybersecurity should also read this short memo from the U.S. Department of Homeland Security’s National Cybersecurity and Communications Integration Center (NCCIC).

[i]Highlights include:

- Elevate cybersecurity risk management discussions to the executive leadership team.
- Implement industry standards and best practices rather than relying solely on compliance standards or certifications.
- Evaluate and manage organization-specific cybersecurity risks.
- Ensure cybersecurity risk metrics are meaningful and measurable.

- Develop and exercise cybersecurity plans and procedures for incident response, business continuity, and disaster recovery.
- Retain a quality workforce.
- Maintain situational awareness of cybersecurity threats.

There is argument to be made that a strong State cybersecurity posture, particularly one that extends to business and critical infrastructure with public/private partnership, could be an economic competitive advantage. But regardless of potential “upside”, the “downside” is very real: “Failure to defend against cyber-attacks can result in more than monetary losses and networked systems damage. When critical systems at hospitals, police, and fire departments are attacked, public safety and individual welfare are at risk (not to mention the exposure of highly sensitive data). Government agencies that are already strapped for financial and IT staff resources can ill afford the time- and labor-intensive recovery process that often follows”.

[i] Reference: Quotes, recent events, and other content sourced from https://statescoop.com/