Cybersecurity Risk Management - Assessment, Mitigation, and Process

Who: The Agency of Digital Services.

What: Conduct a Cyber risk assessment and establish a risk management program.

Where: Entire digital presence for State of Vermont networks and systems.

When: During the next six months (6/20-12/20).

Why: Summary:

Four decades of organic growth has left the State of Vermont with vulnerable systems that still perform critical functions and complex security solutions which in turn increases the workload for staff while still having potential gaps. The massive increase in remote work, due to Covid-19 strains the ability of the Agency to perform deliberate risk-based decision making.

Detail:

The State of Vermont's networks and systems have been built and developed over the course of four decades. Many systems, once in place, remain in a configuration that is grounded in the time they were created. Subsequent, interconnected systems are installed to the lowest risk profile necessary that still allows the systems to communicate. While this situation allows the State to continue to build and improve our technical offerings, over time we end up with systems that are time-locked at a certain level; unable to be upgraded, unfeasible to replace, with an increased risk profile as exploits and technologies improve, but the State systems do not. For example, one Department uses an old ticketing system to manage processes that are critical to their operations. The software platform is multiple versions old and cannot be upgraded without significant expense and disruption to the business process. The old version of the software requires an older server operating system that cannot be upgraded without rendering the software platform inoperable. The server operating system is years beyond its manufacturer's end of life (EOL), in other words, no patches or security updates have been applied since EOL as they are not available from the manufacturer. This server has one of the highest levels of risk of any server in our inventory due to the following reasons:

- **Lack of security patches –** Ensures a vulnerable server becomes increasingly more vulnerable
- **Interconnected system –** A vulnerable server provides a weak link to be exploited in the network and makes other servers more vulnerable due to levels of trust
- **Lack of compliance –** Our Federal partners require that any system that touches data within their compliance model, conforms to their security requirements. Unpatched systems create a "red flag" moment for regulators that affects our ability to maintain status as a trusted partner.
- **Allocation of resources –** More time, energy, and money are spent to maintain this system and to attempt to protect it through compensatory controls. Additional time spent on one system places other systems in jeopardy.

- **Outdated applications –** This catch-all risk addresses the multiple applications that are required to be older and out of date that reside on the server. The server operating system aside, each of the older applications can cause an opening for intrusion into the network.

This is one of many vulnerable systems within our architecture, but system vulnerabilities do not encompass the entirety of our risk. One factor is the patchwork of security and support systems that the State employs to protect systems and data. As Cybersecurity becomes more integrated into daily technical and business operations, manufacturers of security systems and solutions have increased integrations between differing technical solutions. As many offer entire ecosystems of interconnected systems and solutions to protect an enterprise network from the internet down to the end-user device on the desktop. While the systems in place for the State currently provide decent protection, identifying gaps in Cybersecurity is becoming more difficult without adding more solutions that often have overlapping features. This manifests its challenges through both the inefficiencies of having multiple systems to manage and the staff with the expertise to implement the systems. This is in addition to the incomplete usage of the feature sets bundled into the cost of the solutions. As an example, we currently have three solutions that provide threat intelligence (information about adversaries) and we use all three to ensure that we do not miss any knowable threats to our environment. However, we do not have the staff or the automated systems that would help us rapidly identify and act on the large volume of threat data we receive.

The recent change in our circumstances due to the Covid-19 outbreak, have seen the State workforce move outside our “perimeter” and increased the amount of traffic moving into our environment. Remote access requirements, at this scale, require a re-evaluation of our network security and all interconnected systems to address the possibilities of denial of access, network intrusions, and data loss.

Proposal

Summary:

The Agency will hire a third-party vendor to use a standards-based approach to a comprehensive Cybersecurity risk management program. The activities will include risk identification, remediation, and documentation with the goal of a process that will facilitate risk-based decision-making and risk management.

Detail:

The Agency of Digital Services will contract with a third-party to perform a top to bottom assessment of risk across all policies and standards, business practices, and technical systems within its area of responsibility and authority. The engagement will continue with risk mitigation both through internal and vendor-supported means and finally will produce a risk management plan and program to ensure that the Agency can continue to support State systems in an efficient and measured approach. The goal of this engagement is a process that provides for continuous improvement. The key to this approach will be understanding the critical systems (crown jewels) that form the very core of the services the State provides. The assessment will be based on the

NIST Cybersecurity Framework (CSF) which provides an organization with a standards-based approach to cybersecurity and aligns State goals with our Federal partners and many other states. The activities within the CSF are:

- **Identify –** Develop an understanding of risk to systems, people, assets, data, and capabilities.
- **Protect –** Implement appropriate safeguards and security controls to protect critical assets against cyber threats.
- **Detect –** Use continuous security monitoring to spot events that could endanger data or systems.
- **Respond –** Act against detected cybersecurity incidents through established plans covering communications, incident response, analysis, and mitigation.
- **Recover –** Restore any lost capabilities as the result of an incident, in a timely, orderly, and deliberate manner.

The Agency experiences training and proficiency issues when attempting to recruit additional security staff. Often, this is the result of the patchwork of systems and the complexity of the operation not lending itself to finding the specialized staff and leaving it unable to use talent from the higher education pipeline. By using a vendor to perform the majority of the assessment, remediation, and documentation tasks, established security personnel can continue to maintain the systems as they have been established and learn new procedures and systems during the period of the engagement. When the engagement is complete, cybersecurity systems will be working under optimal configurations and will lend themselves to an industry standards-based approach that should help to recruit employees from other industries as well as the higher education pipeline of students.