Anthony Wayne Cyber Security

Chris Hamady

Director of Technology

House Bill 96

HB96 Requires:

1. Cybersecurity Program
2. Incident Reporting
3. Ransomware Approvals
4. Adopt an AI Policy

When Designing a Cyber Security Plan:

1. Risk vs Usability
2. Continuous adaptation

Consider the risks when creating a **balanced** plan that focuses on **increased security** as well as the **usability** of our team member's workplace experiences with their technology implementations.

A cyber security plan is an organic, ever changing, adapting, growing plan that will continually be adjusted and modified to the ever increasing changes and threats as they develop in the world of information technology.

What is NIST?

National Institute of Standards and Technology (NIST) is a non-regulatory U.S. federal agency within the Department of Commerce that promotes innovation and industrial competitiveness by advancing measurement science, standards, and technology.

Six Components of a NIST Cyber Security Plan

1. Identify critical functions and risks
2. Assess the potential impact of breaches
3. Implement threat detection mechanisms
4. Establish incident response procedures
5. Plan for recovery and continuity
6. Define employee training requirements

1. Identify critical functions and risks

- All buildings
- All departments
- All data
- All systems
- All stakeholders

2. Assess the potential impact of breaches

If X is breached, what possible outcomes can potentially happen as a result?

3. Implement threat detection mechanisms

4. Establish incident response procedures

Formulate a plan to determine conclusively what the breached/affected system is: software, hardware, bank accounts, payroll software, etc. and determine:
Should someone be notified? Who should be notified? In what order should the appropriate parties be notified?
What else should be done to recover from this situation? Hardware recovery? Software recovery? Third party systems?

5. Plan for recovery and continuity

Detail the specific plans to recover data and systems so that they can more easily and effectively be implemented, thus getting the District resources back to normal as quickly as possible, and formulate a better plan for the future.

Review, revise, retrain.

6. Define employee training requirements

Plan for annual/quarterly training that focuses on best practice work habits that ultimately lead to the safe, effective use of any and all District technology, data, and systems.

Questions?