
# Cyber Resilience at SNHD

Introduction to core concepts of cyber security including threat landscape, vulnerabilities, controls and best practices.

Cybersecurity and cyber resilience are related concepts but they focus on different aspects of protecting digital assets and systems:

**Cybersecurity** primarily focuses on preventing, detecting, and responding to threats and attacks on digital systems, networks, and data. It encompasses measures such as firewalls, antivirus software, encryption, access controls, and security policies. The main goal of cybersecurity is to reduce the risk of unauthorized access, data breaches, theft, and damage to digital assets.

**Cyber resilience** goes beyond just preventing and detecting cyber threats. It emphasizes the ability of an organization to withstand, adapt to, and quickly recover from cyber attacks or incidents. The goal of cyber resilience is to ensure that ***when*** a cyber attack occurs, the organization can continue to operate effectively and recover as quickly as possible with minimal disruption.

# Current Threats

### Ransomware attacks

Ransomware encrypts data and demands payment for decryption key. Driven by crypto currencies enabling anonymous payments.

### Phishing attacks

Fraudulent emails designed to trick users to disclose credentials or install malware. Education is key to prevention.

### **Social Engineering**

Manipulation of individuals to gain unauthorized access to systems, data, or networks. These attacks exploit human psychology rather than technical vulnerabilities.

Cyber-attacks against government agencies and public sector services are up 40% in the second quarter of 2023 compared to the first.

# SNHD Cyber Resilience Strategy

### Being aware of and managing cyber risks

Identify, Protect, and Monitor all aspects of IT infrastructure and applications.

### Building resilience into systems and operations

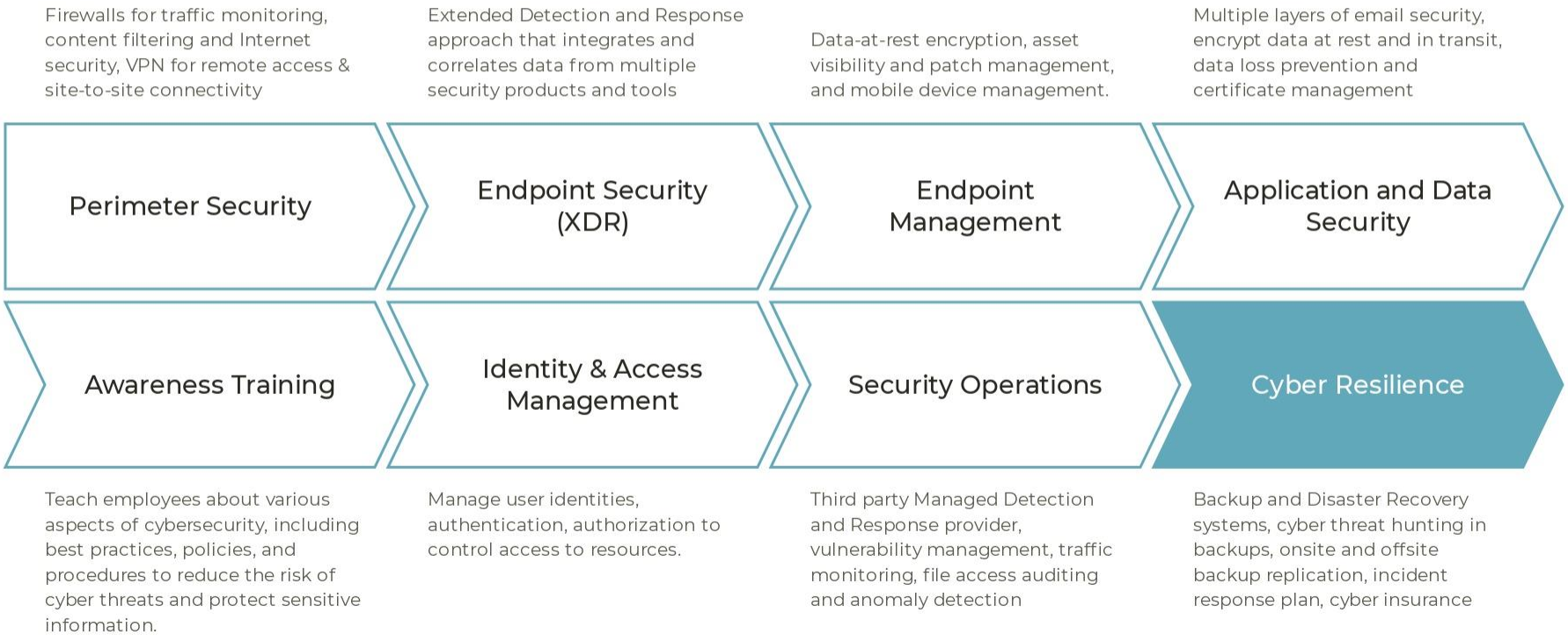
Design systems and operations with security in mind as well as improve our ability to recover from attacks.

### Improving incident response plan

Update our response plan to respond quickly and effectively to any cyberattacks, to restore services for employees and the public.

To accomplish this, we have deployed a robust portfolio of cybersecurity technologies and resiliency solutions.

# Cyber Resilience Areas of Focus



# 2024 Cyber Resilience Priorities

### Develop Resilience Committee

Trained professionals from multiple disciplines that will evaluate cyber security concerns and provide recommendations

### Improve Incident Response Plan

Conduct a vulnerability assessment with a third-party specialist, and implement recommendations

### Focus on Cyber Hygiene

Adopting behaviors and habits throughout the District that promote the security, integrity, and confidentiality of digital assets and information.

We plan on strengthening our resilience and continuity of operations throughout the next few years beginning with the above priorities.