VILLAGE OF SCHAUMBURG

PROGRESS THROUGH THOUGHTFUL PLANNING

Cybersecurity Strategies

Peter Schaak
Director of Information Technology
Village of Schaumburg

Thought Exercise

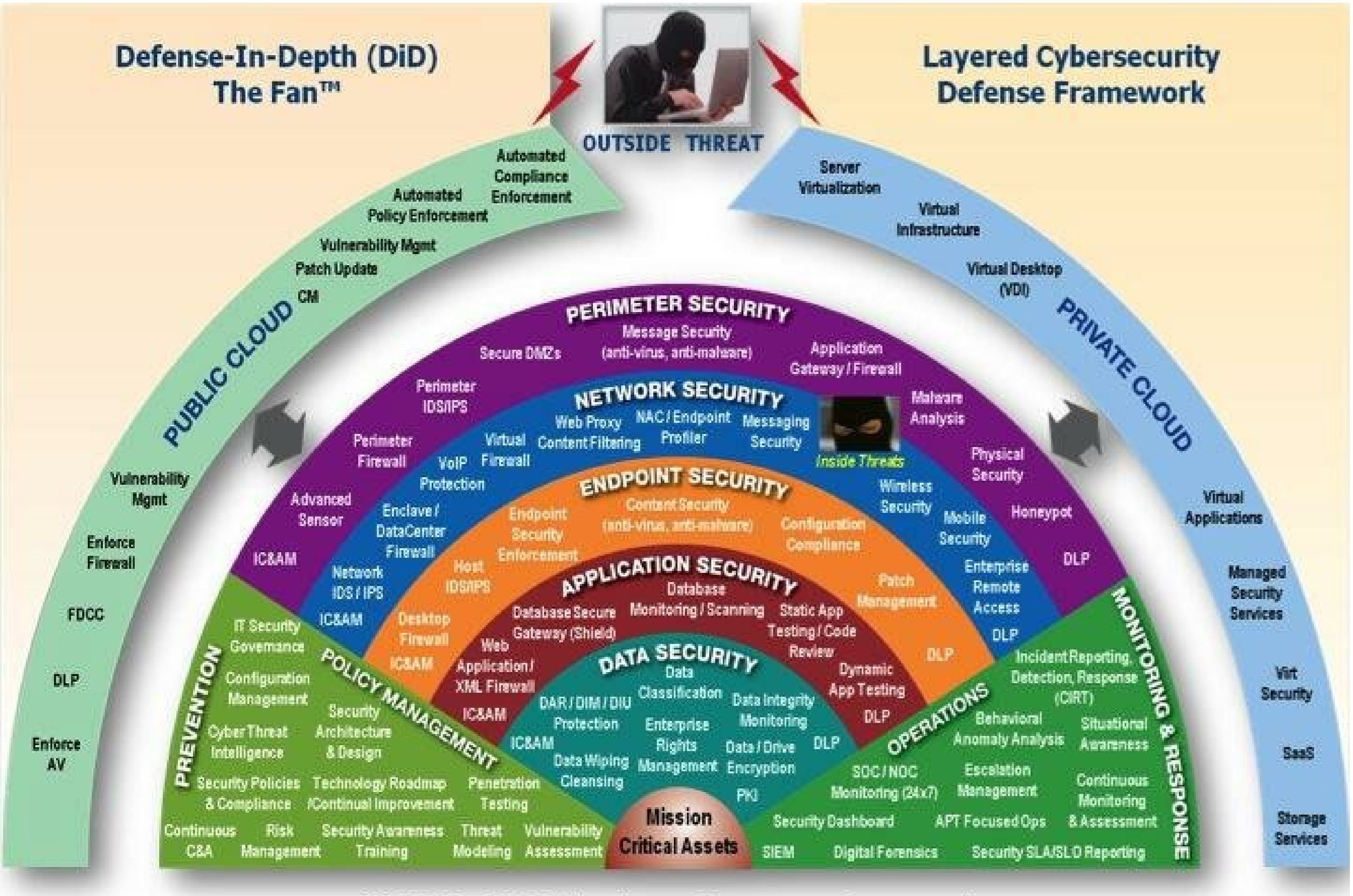
If you received a call right now from your CIO/IT Director telling you your organization has been hacked, do you know your next 5-10-100 steps?

- Who will you call for assistance?
  - Do you have contact info
- Who do you need to notify?
- Who can help us right now?
- How much is this going to cost?
- What critical data do we store?
- What systems are critical for operations?
- What systems need to be addressed first?
- Do we have manual processes for critical activities?
- ...

Two Lanes

1. Prevention
2. Response

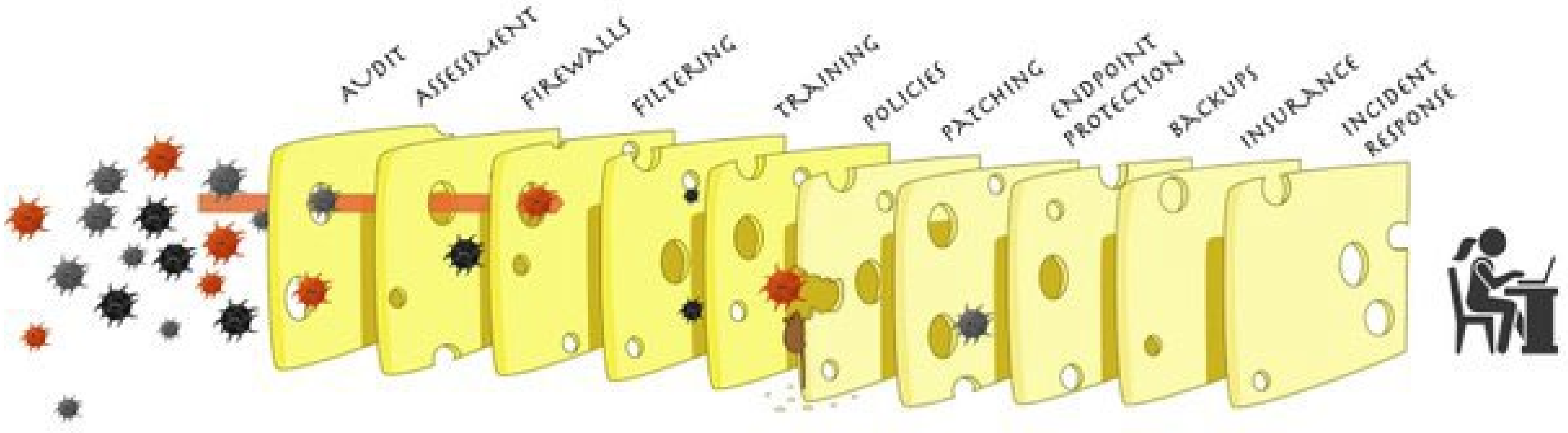
Defense-In-Depth Model



Defense-In-Depth Model

THE SWISS CHEESE CYBERSECURITY DEFENSE-IN-DEPTH MODEL

RECOGNIZING THAT NO SINGLE INTERVENTION IS SUFFICIENT TO PREVENT HARM



EACH INTERVENTION (LAYER) HAS IMPERFECTIONS (HOLES).
MULTIPLE LAYERS IMPROVE SUCCESS.

ADAPTED FROM THE SWISS CHEESE RESPIRATORY VIRUS
PANDEMIC DEFENSE
IAN M. MACKAY VIROLOGYDOWNUNDER.COM

Prevention-Things You Should Be Doing Now…

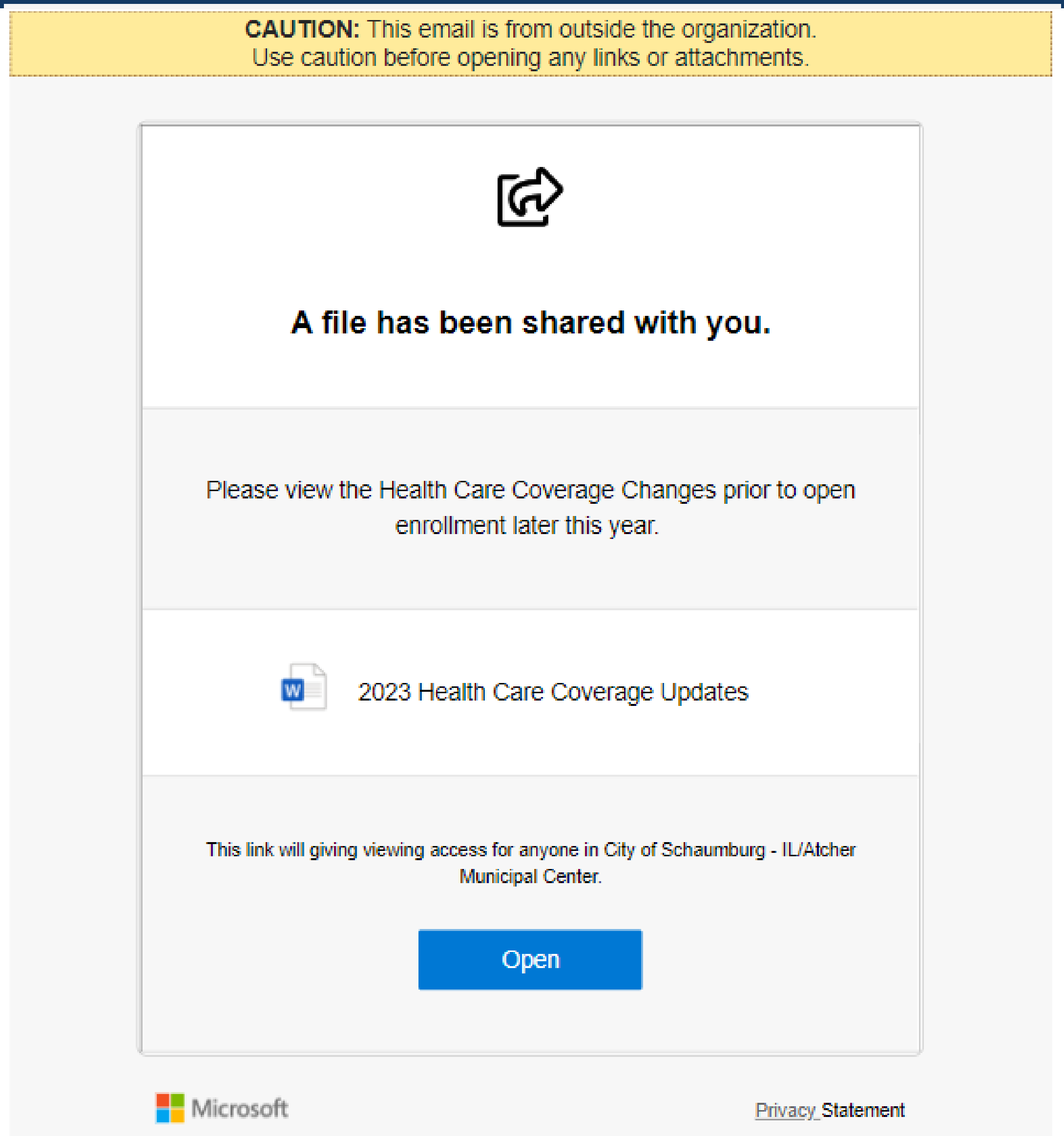
- Prevention
  - System Hardening

Prevention-System Hardening

- EMS-End-Point Management System-Anti-virus, anti-malware everywhere
- IDS-Intrusion Detection Systems-Monitors network traffic for anomalies and DDoS attacks. Sends alerts.
- IDR-Intrusion Detection and Response-Automates detection and response to unusual activity
- Multi-Factor Authentication-Something you know and something you have
- User Authentication Controls
- Access Controls-ID card system

Prevention-Things You Should Be Doing Now...

- Prevention
  - System Hardening
  - Create a sense of paranoia
    - Mock phishing attack



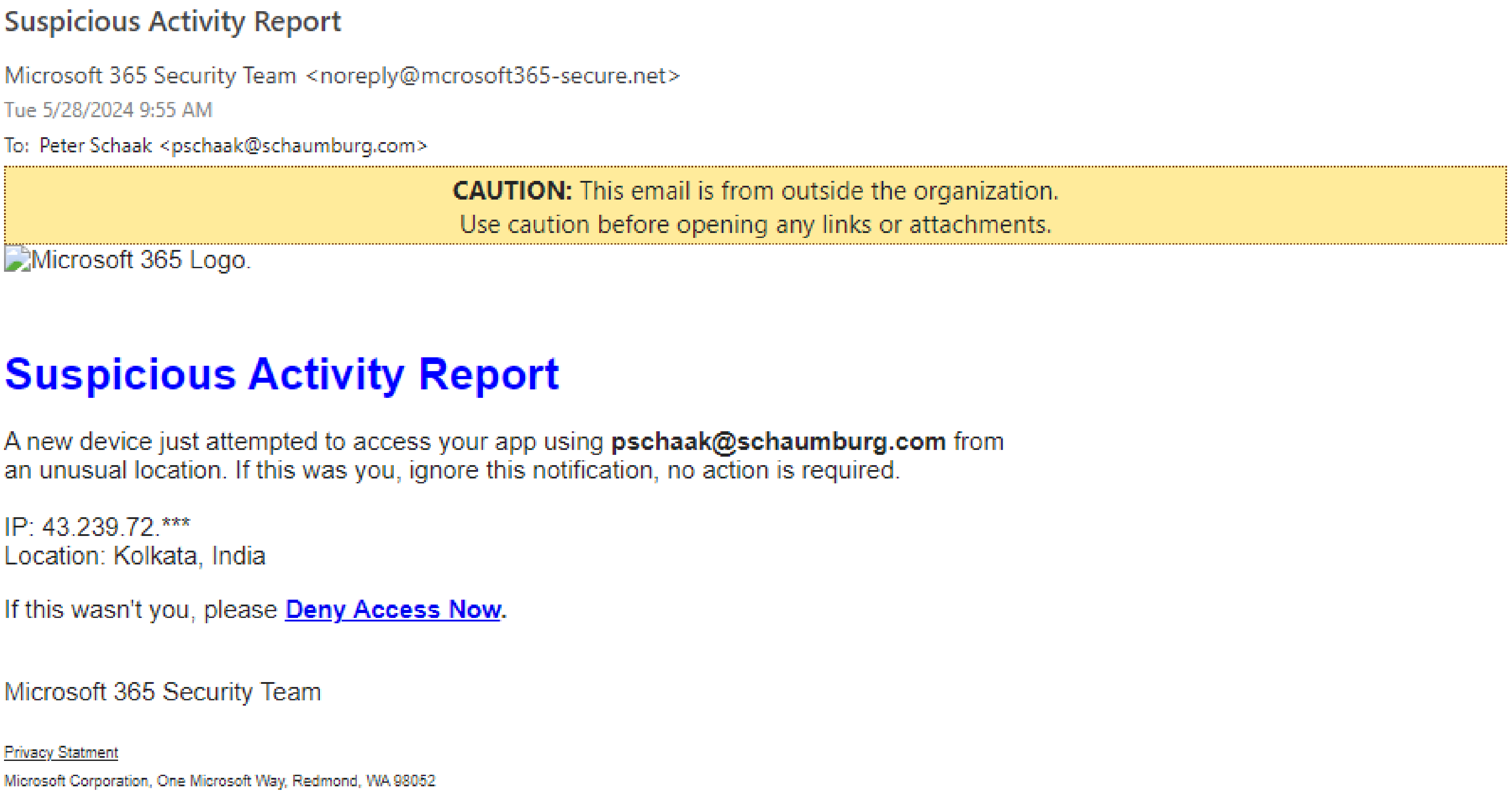
CAUTION: This email is from outside the organization.
Use caution before opening any links or attachments.

A file has been shared with you.

Please view the Health Care Coverage Changes prior to open enrollment later this year.

2023 Health Care Coverage Updates

This link will giving viewing access for anyone in City of Schaumburg - IL/Atcher Municipal Center.



Suspicious Activity Report

Microsoft 365 Security Team <noreply@mcrosoft365-secure.net>
Tue 5/28/2024 9:55 AM
To: Peter Schaak <pschaak@schaumburg.com>

CAUTION: This email is from outside the organization.
Use caution before opening any links or attachments.

Microsoft 365 Logo.

Suspicious Activity Report

A new device just attempted to access your app using **pschaak@schaumburg.com** from an unusual location. If this was you, ignore this notification, no action is required.

IP: 43.239.72.***
Location: Kolkata, India

If this wasn't you, please Deny Access Now.

Microsoft 365 Security Team

Privacy Statment

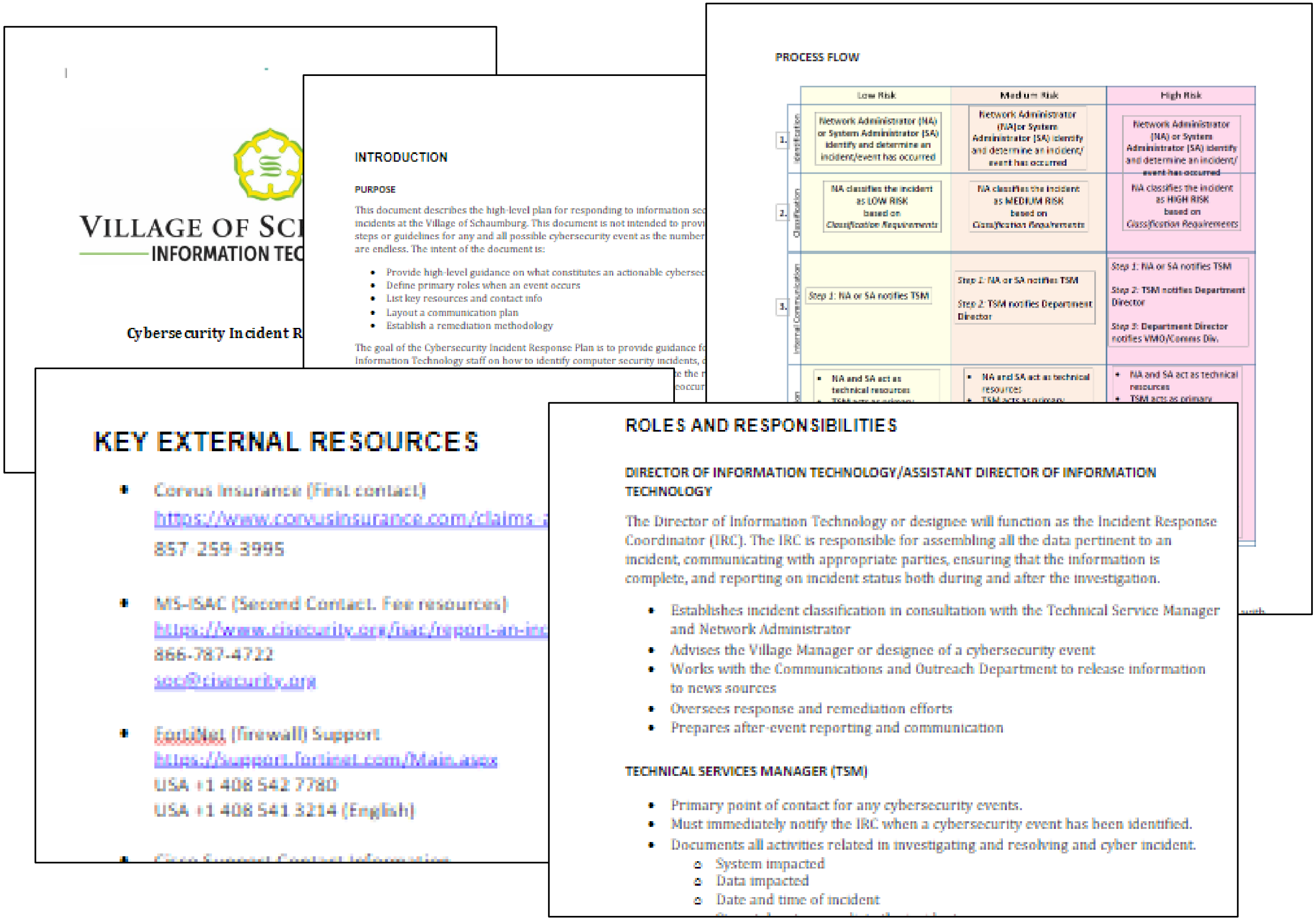
Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Response-Things You Should Be Doing Now...

- Prevention
  - System Hardening
  - Create a sense of paranoia
    - Mock phishing attack
- Response
  - Incident Response Plan

Response-Incident Response Plan

Village of Schaumburg
PROGRESS THROUGH THOUGHTFUL PLANNING



Village of Sc
INFORMATION TEC

Cybersecurity Incident R

INTRODUCTION

PURPOSE

This document describes the high-level plan for responding to information sec
incidents at the Village of Schaumburg. This document is not intended to provi
steps or guidelines for any and all possible cybersecurity event as the number
are endless. The intent of the document is:

- Provide high-level guidance on what constitutes an actionable cybersec
- Define primary roles when an event occurs
- List key resources and contact info
- Layout a communication plan
- Establish a remediation methodology

The goal of the Cybersecurity Incident Response Plan is to provide guidance fo
Information Technology staff on how to identify computer security incidents, d
te the r
eoccur

PROCESS FLOW

		Low Risk	Medium Risk	High Risk
1.	Identification	Network Administrator (NA) or System Administrator (SA) identify and determine an incident/event has occurred	Network Administrator (NA)or System Administrator (SA) identify and determine an incident/ event has occurred	Network Administrator (NA) or System Administrator (SA) identify and determine an incident/ event has occurred
2.	Classification	NA classifies the incident as LOW RISK based on *Classification Requirements*	NA classifies the incident as MEDIUM RISK based on *Classification Requirements*	NA classifies the incident as HIGH RISK based on *Classification Requirements*
3.	Internal Communication	*Step 1:* NA or SA notifies TSM	*Step 1:* NA or SA notifies TSM *Step 2:* TSM notifies Department Director	*Step 1:* NA or SA notifies TSM *Step 2:* TSM notifies Department Director *Step 3:* Department Director notifies VMO/Comms Div.
		• NA and SA act as technical resources • TSM acts as primary	• NA and SA act as technical resources • TSM acts as primary	• NA and SA act as technical resources • TSM acts as primary

KEY EXTERNAL RESOURCES

- Corvus Insurance (First contact)
  https://www.corvusinsurance.com/claims
  857-259-3995

- MS-ISAC (Second Contact. Fee resources)
  https://www.cisecurity.org/isac/report-an-inc
  866-787-4722
  soc@cisecurity.org

- FortiNet (firewall) Support
  https://support.fortinet.com/Main.aspx
  USA +1 408 542 7780
  USA +1 408 541 3214 (English)

- Cisco Support Contact Information

ROLES AND RESPONSIBILITIES

DIRECTOR OF INFORMATION TECHNOLOGY/ASSISTANT DIRECTOR OF INFORMATION TECHNOLOGY

The Director of Information Technology or designee will function as the Incident Response Coordinator (IRC). The IRC is responsible for assembling all the data pertinent to an incident, communicating with appropriate parties, ensuring that the information is complete, and reporting on incident status both during and after the investigation.

- Establishes incident classification in consultation with the Technical Service Manager and Network Administrator
- Advises the Village Manager or designee of a cybersecurity event
- Works with the Communications and Outreach Department to release information to news sources
- Oversees response and remediation efforts
- Prepares after-event reporting and communication

TECHNICAL SERVICES MANAGER (TSM)

- Primary point of contact for any cybersecurity events.
- Must immediately notify the IRC when a cybersecurity event has been identified.
- Documents all activities related in investigating and resolving and cyber incident.
  - System impacted
  - Data impacted
  - Date and time of incident

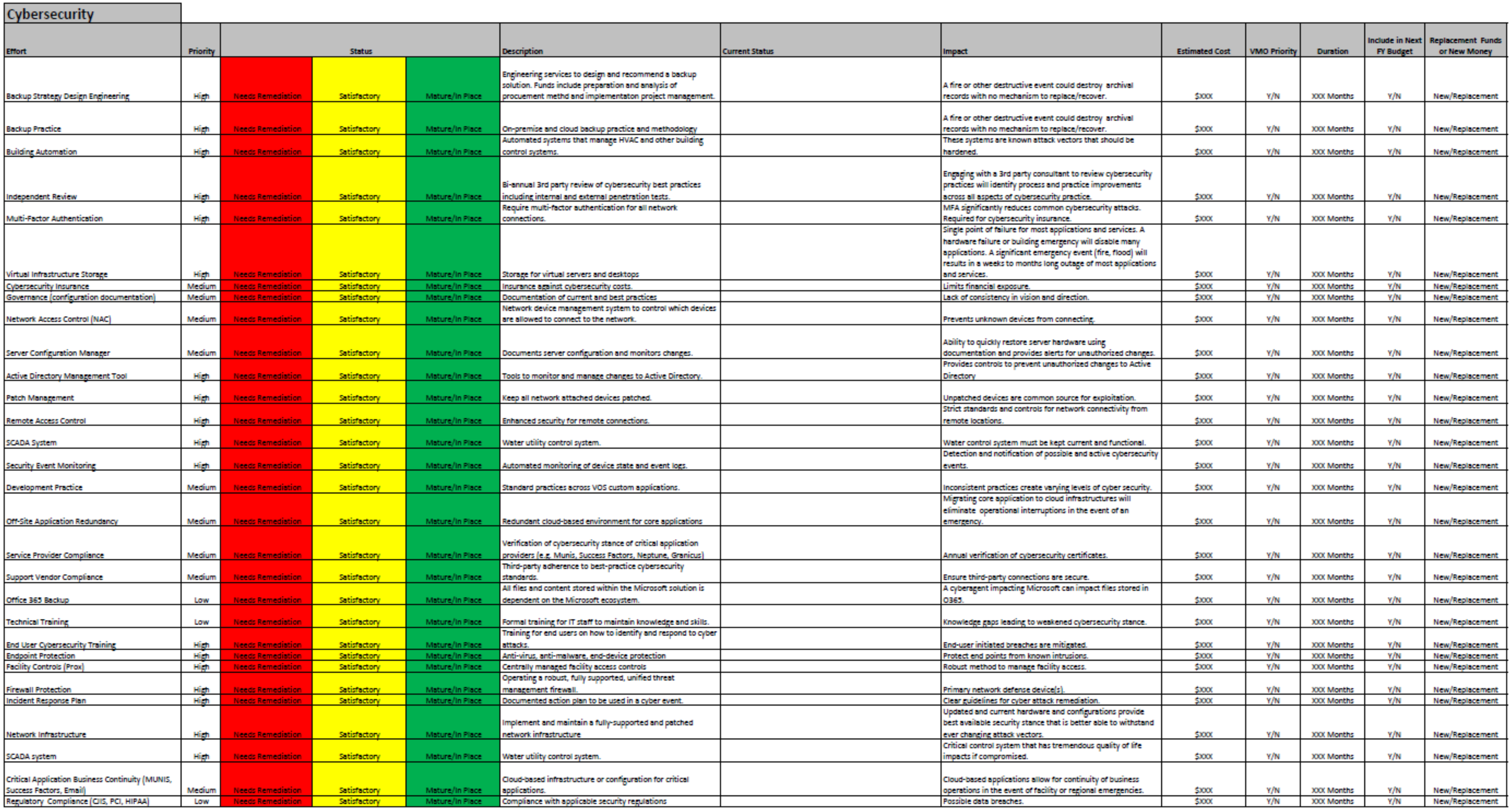
Response-Things You Should Be Doing Now...

VILLAGE OF SCHAUMBURG
PROGRESS THROUGH THOUGHTFUL PLANNING

- Prevention
  - System Hardening
  - Create a sense of paranoia
    - Mock phishing attack
- Response
  - Incident Response Plan
  - Cybersecurity Report Card

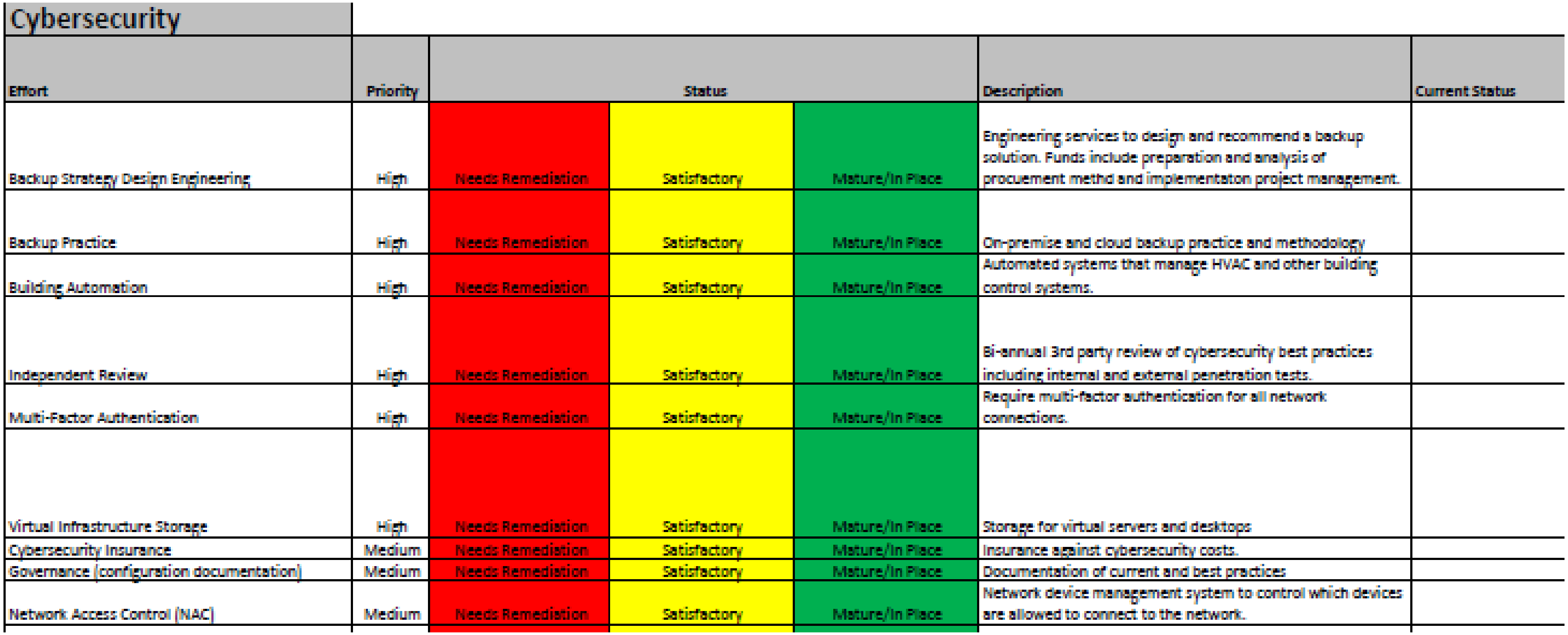
Response-Cybersecurity Report Card

VILLAGE OF SCHAUMBURG
PROGRESS THROUGH THOUGHTFUL PLANNING



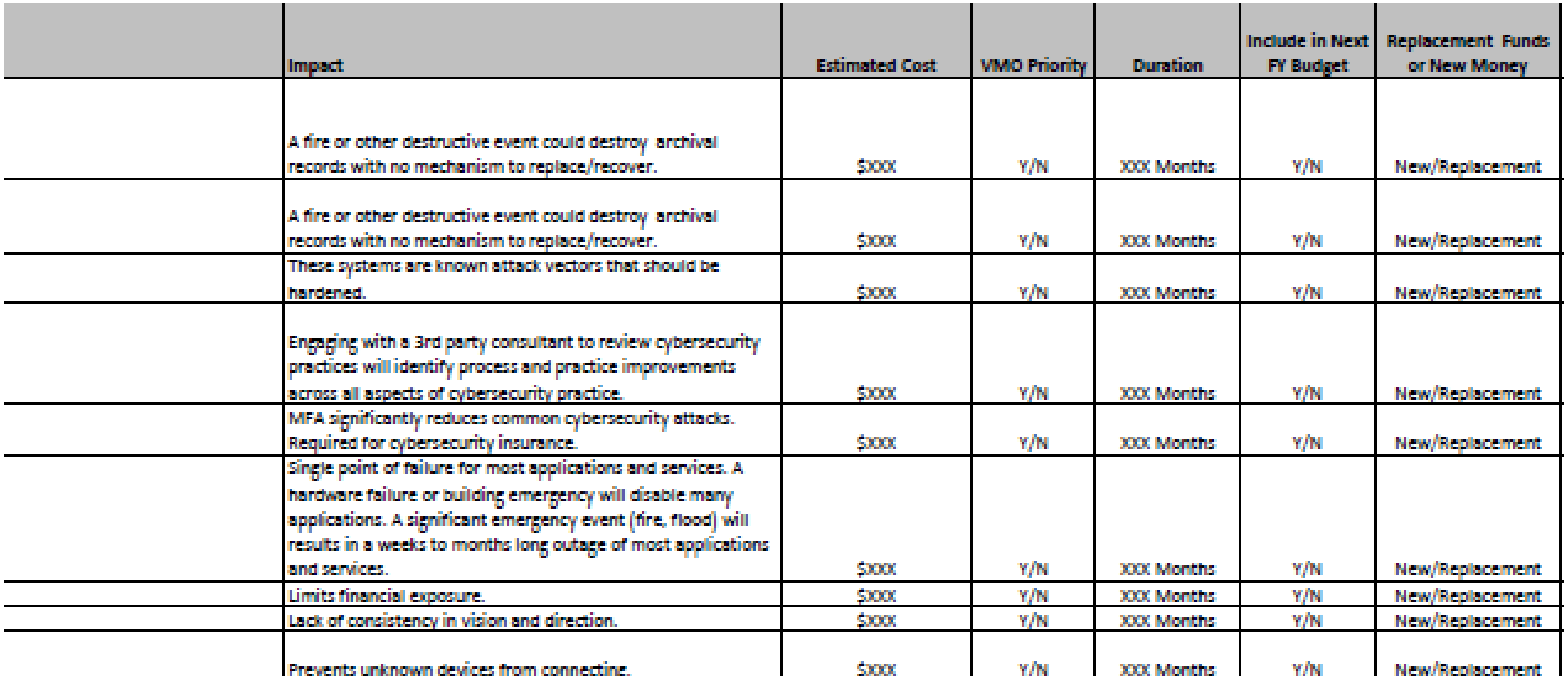
Cybersecurity

Effort	Priority	Status			Description	Current Status	Impact	Estimated Cost	VMO Priority	Duration	Include in Next FY Budget	Replacement Funds or New Money
Backup Strategy Design Engineering	High	Needs Remediation	Satisfactory	Mature/In Place	Engineering services to design and recommend a backup solution. Funds include preparation and analysis of procuement methd and implementaton project management.		A fire or other destructive event could destroy archival records with no mechanism to replace/recover.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Backup Practice	High	Needs Remediation	Satisfactory	Mature/In Place	On-premise and cloud backup practice and methodology		A fire or other destructive event could destroy archival records with no mechanism to replace/recover.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Building Automation	High	Needs Remediation	Satisfactory	Mature/In Place	Automated systems that manage HVAC and other building control systems.		These systems are known attack vectors that should be hardened.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Independent Review	High	Needs Remediation	Satisfactory	Mature/In Place	Bi-annual 3rd party review of cybersecurity best practices including internal and external penetration tests.		Engaging with a 3rd party consultant to review cybersecurity practices will identify process and practice improvements across all aspects of cybersecurity practice.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Multi-Factor Authentication	High	Needs Remediation	Satisfactory	Mature/In Place	Require multi-factor authentication for all network connections.		MFA significantly reduces common cybersecurity attacks. Required for cybersecurity insurance.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Virtual Infrastructure Storage	High	Needs Remediation	Satisfactory	Mature/In Place	Storage for virtual servers and desktops		Single point of failure for most applications and services. A hardware failure or building emergency will disable many applications. A significant emergency event (fire, flood) will results in a weeks to months long outage of most applications and services.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Cybersecurity Insurance	Medium	Needs Remediation	Satisfactory	Mature/In Place	Insurance against cybersecurity costs.		Limits financial exposure.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Governance (configuration documentation)	Medium	Needs Remediation	Satisfactory	Mature/In Place	Documentation of current and best practices		Lack of consistency in vision and direction.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Network Access Control (NAC)	Medium	Needs Remediation	Satisfactory	Mature/In Place	Network device management system to control which devices are allowed to connect to the network.		Prevents unknown devices from connecting.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Server Configuration Manager	Medium	Needs Remediation	Satisfactory	Mature/In Place	Documents server configuration and monitors changes.		Ability to quickly restore server hardware using documentation and provides alerts for unauthorized changes.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Active Directory Management Tool	High	Needs Remediation	Satisfactory	Mature/In Place	Tools to monitor and manage changes to Active Directory.		Provides controls to prevent unauthorized changes to Active Directory	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Patch Management	High	Needs Remediation	Satisfactory	Mature/In Place	Keep all network attached devices patched.		Unpatched devices are common source for exploitation.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Remote Access Control	High	Needs Remediation	Satisfactory	Mature/In Place	Enhanced security for remote connections.		Strict standards and controls for network connectivity from remote locations.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
SCADA System	High	Needs Remediation	Satisfactory	Mature/In Place	Water utility control system.		Water control system must be kept current and functional.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Security Event Monitoring	High	Needs Remediation	Satisfactory	Mature/In Place	Automated monitoring of device state and event logs.		Detection and notification of possible and active cybersecurity events.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Development Practice	Medium	Needs Remediation	Satisfactory	Mature/In Place	Standard practices across VOS custom applications.		Inconsistent practices create varying levels of cyber security.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Off-Site Application Redundancy	Medium	Needs Remediation	Satisfactory	Mature/In Place	Redundant cloud-based environment for core applications		Migrating core application to cloud infrastructures will eliminate operational interruptions in the event of an emergency.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Service Provider Compliance	Medium	Needs Remediation	Satisfactory	Mature/In Place	Verification of cybersecurity stance of critical application providers (e.g. Munis, Success Factors, Neptune, Granicus)		Annual verification of cybersecurity certificates.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Support Vendor Compliance	Medium	Needs Remediation	Satisfactory	Mature/In Place	Third-party adherence to best-practice cybersecurity standards.		Ensure third-party connections are secure.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Office 365 Backup	Low	Needs Remediation	Satisfactory	Mature/In Place	All files and content stored within the Microsoft solution is dependent on the Microsoft ecosystem.		A cyberagent impacting Microsoft can impact files stored in O365.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Technical Training	Low	Needs Remediation	Satisfactory	Mature/In Place	Formal training for IT staff to maintain knowledge and skills.		Knowledge gaps leading to weakened cybersecurity stance.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
End User Cybersecurity Training	High	Needs Remediation	Satisfactory	Mature/In Place	Training for end users on how to identify and respond to cyber attacks.		End-user initiated breaches are mitigated.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Endpoint Protection	High	Needs Remediation	Satisfactory	Mature/In Place	Anti-virus, anti-malware, end-device protection		Protect end points from known intrusions.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Facility Controls (Prox)	High	Needs Remediation	Satisfactory	Mature/In Place	Centrally managed facility access controls		Robust method to manage facility access.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Firewall Protection	High	Needs Remediation	Satisfactory	Mature/In Place	Operating a robust, fully supported, unified threat management firewall.		Primary network defense device(s).	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Incident Response Plan	High	Needs Remediation	Satisfactory	Mature/In Place	Documented action plan to be used in a cyber event.		Clear guidelines for cyber attack remediation.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Network Infrastructure	High	Needs Remediation	Satisfactory	Mature/In Place	Implement and maintain a fully-supported and patched network infrastructure		Updated and current hardware and configurations provide best available security stance that is better able to withstand ever changing attack vectors.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
SCADA system	High	Needs Remediation	Satisfactory	Mature/In Place	Water utility control system.		Critical control system that has tremendous quality of life impacts if compromised.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Critical Application Business Continuity (MUNIS, Success Factors, Email)	Medium	Needs Remediation	Satisfactory	Mature/In Place	Cloud-based infrastructure or configuration for critical applications.		Cloud-based applications allow for continuity of business operations in the event of facility or regional emergencies.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
Regulatory Compliance (CJIS, PCI, HIPAA)	Low	Needs Remediation	Satisfactory	Mature/In Place	Compliance with applicable security regulations		Possible data breaches.	$XXX	Y/N	XXX Months	Y/N	New/Replacement



Cybersecurity

Effort	Priority	Status			Description	Current Status
Backup Strategy Design Engineering	High	Needs Remediation	Satisfactory	Mature/In Place	Engineering services to design and recommend a backup solution. Funds include preparation and analysis of procuement methd and implementaton project management.	
Backup Practice	High	Needs Remediation	Satisfactory	Mature/In Place	On-premise and cloud backup practice and methodology	
Building Automation	High	Needs Remediation	Satisfactory	Mature/In Place	Automated systems that manage HVAC and other building control systems.	
Independent Review	High	Needs Remediation	Satisfactory	Mature/In Place	Bi-annual 3rd party review of cybersecurity best practices including internal and external penetration tests.	
Multi-Factor Authentication	High	Needs Remediation	Satisfactory	Mature/In Place	Require multi-factor authentication for all network connections.	
Virtual Infrastructure Storage	High	Needs Remediation	Satisfactory	Mature/In Place	Storage for virtual servers and desktops	
Cybersecurity Insurance	Medium	Needs Remediation	Satisfactory	Mature/In Place	Insurance against cybersecurity costs.	
Governance (configuration documentation)	Medium	Needs Remediation	Satisfactory	Mature/In Place	Documentation of current and best practices	
Network Access Control (NAC)	Medium	Needs Remediation	Satisfactory	Mature/In Place	Network device management system to control which devices are allowed to connect to the network.	



	Impact	Estimated Cost	VMO Priority	Duration	Include in Next FY Budget	Replacement Funds or New Money
	A fire or other destructive event could destroy archival records with no mechanism to replace/recover.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
	A fire or other destructive event could destroy archival records with no mechanism to replace/recover.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
	These systems are known attack vectors that should be hardened.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
	Engaging with a 3rd party consultant to review cybersecurity practices will identify process and practice improvements across all aspects of cybersecurity practice.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
	MFA significantly reduces common cybersecurity attacks. Required for cybersecurity insurance.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
	Single point of failure for most applications and services. A hardware failure or building emergency will disable many applications. A significant emergency event (fire, flood) will results in a weeks to months long outage of most applications and services.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
	Limits financial exposure.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
	Lack of consistency in vision and direction.	$XXX	Y/N	XXX Months	Y/N	New/Replacement
	Prevents unknown devices from connecting.	$XXX	Y/N	XXX Months	Y/N	New/Replacement

Response-Things You Should Be Doing Now...

- Prevention
  - System Hardening
  - Create a sense of paranoia
    - Mock phishing attack
- Response
  - Incident Response Plan
  - Cybersecurity Report Card
  - Tabletop Exercises
    - Practice, Practice, Practice

Questions??

Thank You!