SVAM INTERNATIONAL, INC.



Partners with Purpose

Driving meaningful change through digital acceleration.

nassau BOCES

© 2024 SVAM. All Rights Reserved.

SVAM INTERNATIONAL, INC.

SVAM is

Insights, Intelligence & Innovation

SVAM is here to deliver **meaningful business value** to our customers through **digital acceleration**. Our expertise is in improving your access to critical data, **automating your business processes**, and enabling your teams to **collaborate effectively**.

With our **entrusted global network of highly experienced** and knowledgeable **technology consultants**, we are committed to exceeding our clients' technology needs with the **highest quality, value-driven software solutions and customized cybersecurity advisory services**.

30+

Years of experience

800+

Employees

25,000+

Network of consultants

© 2024 SVAM. All Rights Reserved.

SVAM
INTERNATIONAL, INC.

Our Solutions

- Cybersecurity
- Digital Transformation
- Enterprise Platforms
- Business Automation with AI
- Data Modernization
- Staff Augmentation



SVAM SOLUTIONS

© 2024 SVAM. All Rights Reserved.

Service

Cybersecurity

Intentional safeguarding of your digital systems, networks, and data from malicious threats and unauthorized access. SVAM's cybersecurity practice **encompasses a wide range of technologies, processes, and practices to protect against cyberattacks**, ensuring the confidentiality, integrity, and availability of sensitive information.

Microsoft rubrik schellman

ninjaOne SentinelOne Acronis

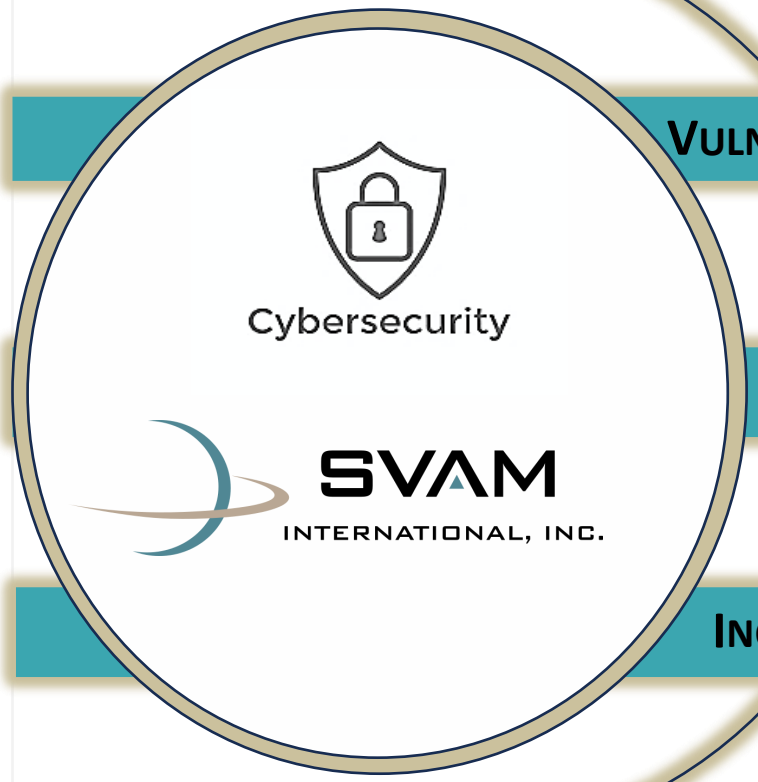
Blumira DUO



© 2024 SVAM. All Rights Reserved.

Results Driven Cybersecurity Services

CYBESECURITY SERVICES



NIST Assessments & Gap Analysis

Identify gaps in your cybersecurity practices, offering a precise analysis and actionable steps to align with NIST standards and strengthen your defenses.

Vulnerability Assessments

Evaluate vulnerabilities across critical IT assets and obtain targeted recommendations that provide measurable results safeguarding your assets from regulatory and cyber risks.

Penetration Testing

Simulate real world cyber-attacks and gain a 360-degree understanding of the security issues and underlying solutions about your existing and emerging technologies across business verticals.

Incident Response Plan

Design and Implement actionable incident response plans tailored to your organization that will provide autonomy with step-by-step procedures to detect, respond to, and mitigate cyber threats.

Third Party Risk Assessments

Take control of your external threat landscape by ensuring your vendors meet your security standards and do not threaten your organization's security posture.

© 2024 SVAM. All Rights Reserved.

Results Driven Cybersecurity Services



CONTINUOUS COMPLIANCE APPROACH

Transition to a continuous compliance approach with automated testing and monitoring of controls in a dynamic environment.

GOVERNANCE & VCISO

Our virtual CISO (vCISO) provides oversight, governance, and strategic plan and defines your cybersecurity strategic objectives aligned with the business objectives and goals.

ZERO TRUST

Build an ecosystem of continuous authentication and authorization, enhancing security in a dynamic environment.

CYBERSECURITY STAFFING

Technical screening supported by global teams within SVAM's Cybersecurity practice. Flexible models including contract, contract-to-hire, try and buy, full-time

IT MANAGED SERVICES PROVIDER

Improve operations, remove costly problems, and optimize how your staff spends their time.

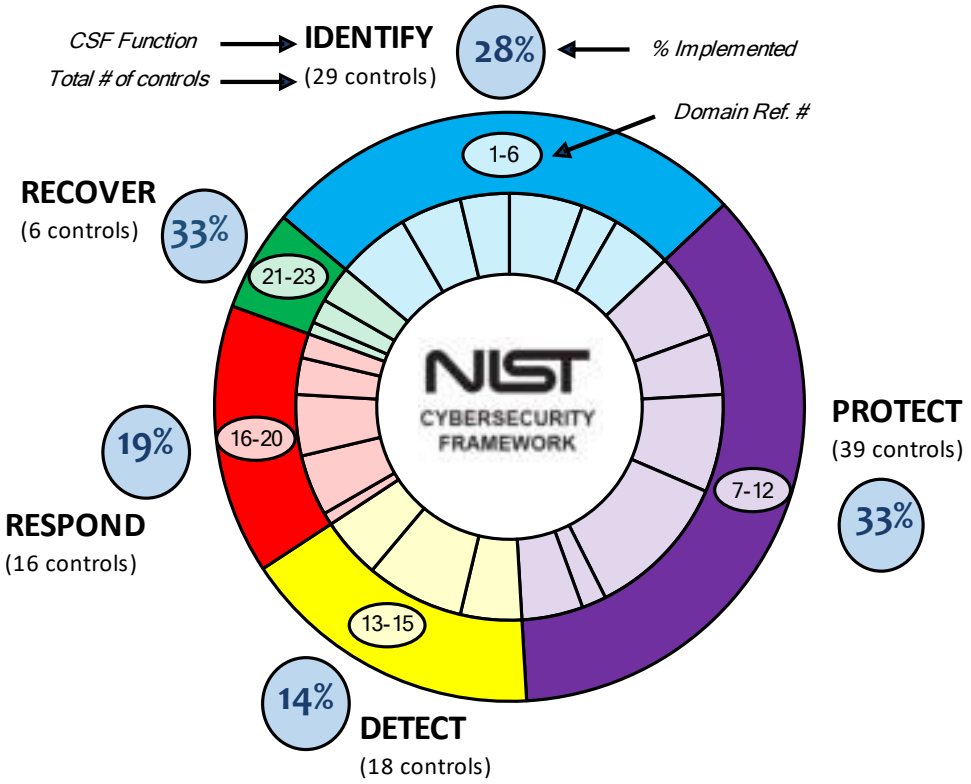
© 2024 SVAM. All Rights Reserved.

NIST CSF Alignment

Based on our review, Client has multiple improvement opportunities in order to be aligned with the NIST CSF controls. Various gaps identified are shared observations for multiple controls which will significantly elevate the alignment once as they are remediated. The following is an illustration of the number of controls that need to be mitigated for each cybersecurity domain:

#	NIST CSF Domains	High Ris	TC	FI	PI	NI
1	Asset Management (ID.AM)	3	6	-	5	1
2	Business Environment (ID.BE)	1	5	-	5	-
3	Governance (ID.GV)	2	4	-	1	3
4	Risk Assessment (ID.RA)	2	6	-	2	4
5	Risk Management Strategy (ID.RM)	3	3	-	1	2
6	Supply Chain Risk Management (ID.SC)	2	5	-	2	3
7	Identity Mgmt., Authentication & Access Control (PR.AC)	4	7	2	4	1
8	Awareness and Training (PR.AT)	3	5	-	2	3
9	Data Security (PR.DS)	4	8	-	3	5
10	Information Protection Processes and Procedures (PR.IP)	2	12	1	5	6
11	Maintenance (PR.MA)	-	2	-	2	-
12	Protective Technology (PR.PT)	1	5	-	4	1
13	Anomalies and Events (DE.AE)	3	5	-	2	3
14	Security Continuous Monitoring (DE.CM)	5	8	-	2	6
15	Detection Processes (DE.DP)	5	5	-	1	4
16	Response Planning (RS.RP)	1	1	-	-	1
17	Communications (RS.CO)	3	5	-	2	3
18	Analysis (RS.AN)	4	5	-	2	3
19	Mitigation (RS.MI)	1	3	-	2	1
20	Improvements (RS.IM)	2	2	-	-	2
21	Recovery Planning (RC.RP)	1	1	-	1	-
22	Improvements (RC.IM)	2	2	-	-	2
23	Communications (RC.CO)	-	3	-	3	-

See table on right (TC, FI, PI, NI)



©2021 SVAM International Inc proprietary, confidential. All rights reserved.

© 2024 SVAM. All Rights Reserved.

High Level Summary of Opportunities for Improvement

Resulting from this assessment, the following areas of opportunities will significantly improve the organization's Cybersecurity Risk Management program:

Security Operations

Centralized Security Operations Center (SOC) to monitor and manage security incidents, identity and access management, and remediate identified vulnerabilities across the organization's environment

Policies & Procedures / Training

Enhanced core policies and procedures related to Asset Management, Incident Response program, Vulnerability Management, Security Operation Center (SOC) & Identity and Access Management Program (IAM)

Continued information security training and awareness programs for all users, including students, parents, employees, & schools

Governance

Enhanced governance, internal & external, including 3rd party vendors and partners

Optimize Resource Requirement

Relative to size & complexity of the organization, optimize resource requirements to fulfill demand & inquiries from various groups (ITSDs, schools, etc.)

Rated Cyber Risk

Identified, risk rated, and prioritized cyber risk mitigation programs aligned with cybersecurity roadmap and ITSD risk profile results, including tactical and immediate areas of focus

Critical & Dependent IT functions

Established critical and foundational processes (sometimes not owned by the CISO organization) that are highly dependent on capability and delivery of services by the organization
Ex. IT Asset Management, application / data inventory and classification

Secure SDLC

Design, build, and run with security requirements and controls earlier throughout the life cycle of application development and production support.

Third-party Risk Management

Improved Third-party risk management program by integrating and aligning various functions, establishing processes for vendor due diligence and monitoring and defining risk ratings for all vendor categories

©2021 SVAM International Inc proprietary, confidential. All rights reserved.

© 2024 SVAM. All Rights Reserved.

Recommended Roadmap Timeline

	#	Task / Phase	Risk Level	Year 1 to Year 2: 0-6 Months	Year 1 to Year 2: 6-18months
●	10	Acquire and implement the capability to collect all system, security, and application logs. Implement policy and procedures to review and analyze events.*	High	X	
★ ●	11	Establish a formal security awareness training program*	High	X	
★	12	Establish a risk management program to identify, manage, and track IT/Cyber and Vendor Risks*	High	X	
●	13	Review all user access in Dropbox and remove all accounts that are not registered through the Enterprise licensing or purchase additional licenses for users who require access*	High	X	
★ ●	14	Perform regular vulnerability scanning and penetration testing (**)	High	X	
★	15	Establish an access management program including a remote user access policy and a control such as formal access reviews in all systems and applications on a regular basis*	High		X
★	16	Formalize an offboarding HR policy that includes timely communication of access terminations	High		X
	17	Review ,update and document firewall rules	High		X
●	18	Monitor user activity with Maas360 using a risk-based approach	High		X

- *Each task may be related to more than one control, including shared controls against NIST
- ** While not specifically assessed, it is expected that organizations continuously perform vulnerability scanning and penetra tion testing exercises regularly

★ *Proposed Phase 2 vCISO Activities*

● *Potential Need for Tech Investment*

©2021 SVAM International Inc proprietary, confidential. All rights reserved.

© 2024 SVAM. All Rights Reserved.

Recommended Roadmap Timeline

Key Finding

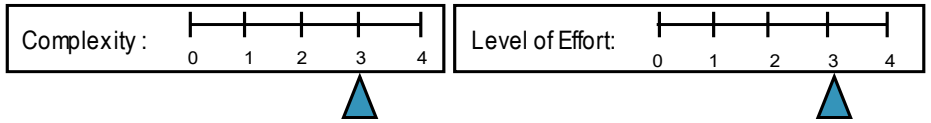
1. XX does not have a cybersecurity risk management function established in place to identify, quantify, prioritize and remediate all cybersecurity risks within the organization. Additionally, XX has not adopted a cybersecurity risk management framework to support their existing enterprise risk management program in order to conduct ongoing cybersecurity risk assessments.
   - Risk: Without a formal risk management function, there is limited visibility into identifying, measuring, mitigating and monitoring IT risk. This may result in inadequate decision-making regarding the implementation of appropriate controls.

Key Recommendati Finding Impact High

1. Management should consider adopting an industry framework, such as the National Institutes of Standardization and Technology (NIST) 800-30 Risk Management Guide for Information Technology Systems, to establish a cybersecurity risk management function.
   - A cybersecurity risk management policy should be documented with requirements and processes for identifying, prioritizing, analyzing, escalating and remediating cybersecurity risks.
   - To support the development of creating a risk management function, XX should maintain a centralized inventory of all cybersecurity risks and prioritize them based on their level of risk to the organization (i.e Risk Register).

Key Finding is Mapped to the Following Risk(s):

Risk Register #	Risk Definition	InitiaRisk	ResiduaRisk
2	IT Risk Management	High (25)	Medium (12)



Owner

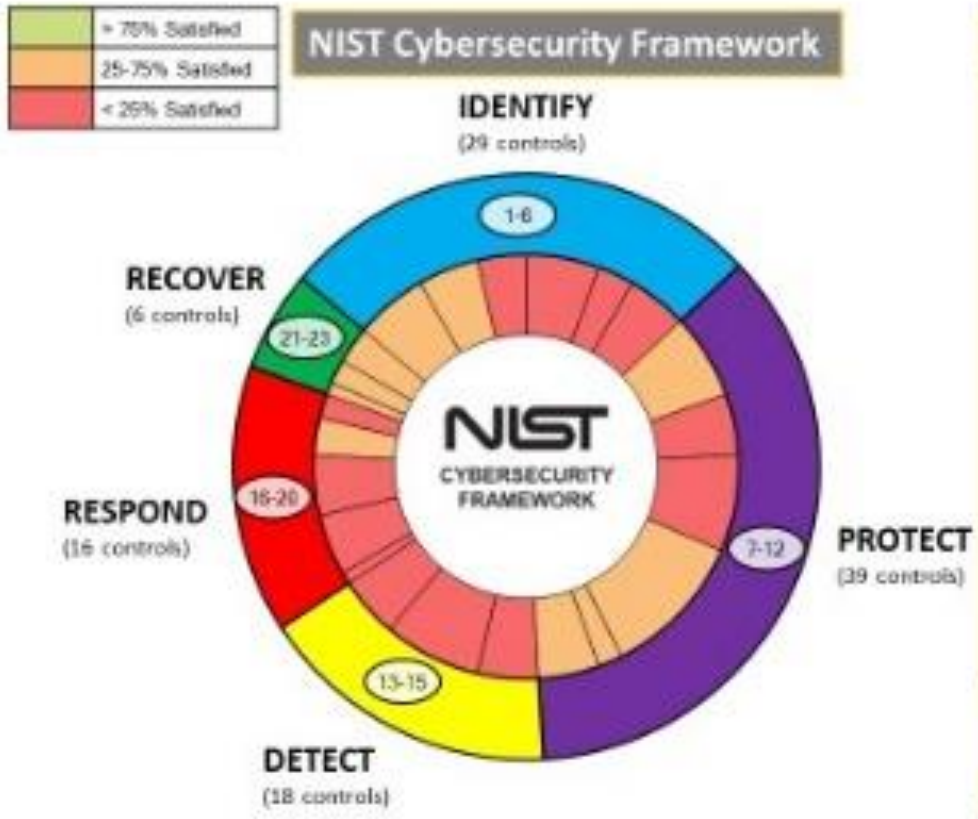
©2021 SVAM International Inc proprietary, confidential. All rights reserved.

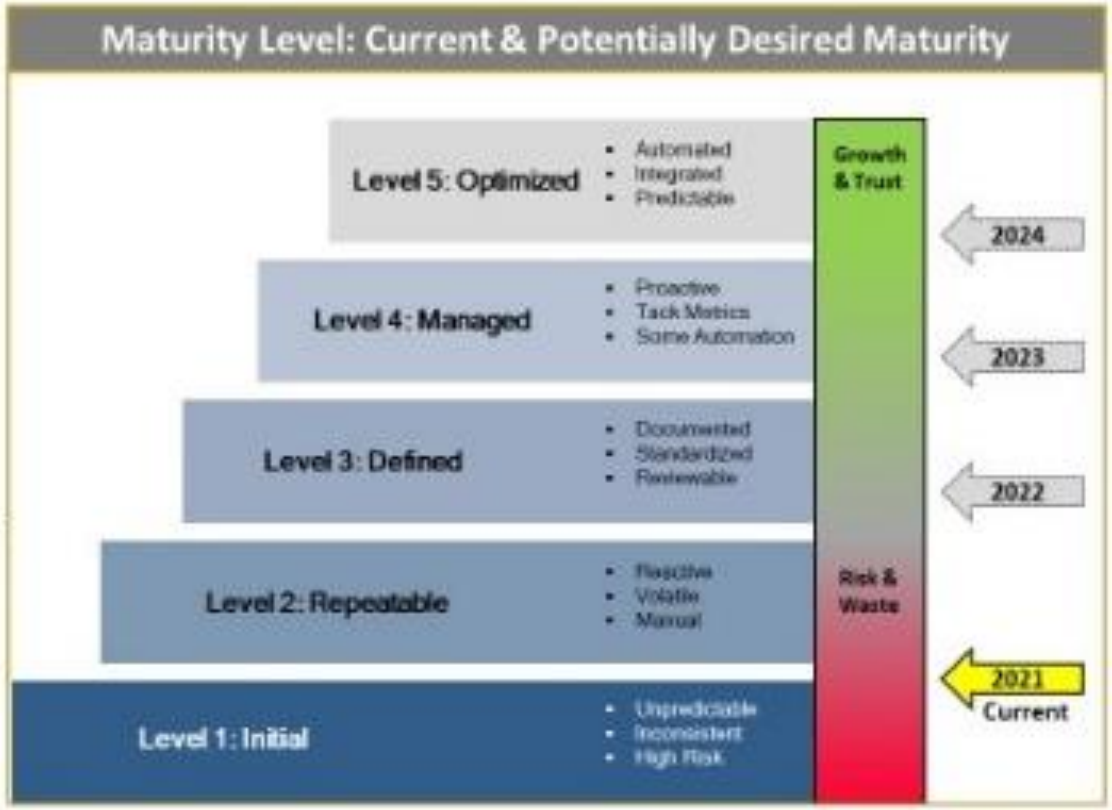
© 2024 SVAM. All Rights Reserved.

SVAM
INTERNATIONAL, INC.

SAMPLE REPORTS

Cybersecurity Maturity





The desired Maturity Level is dependent on the risk appetite of the organization and compliance needs.

©2021 SVAM International Inc proprietary, confidential. All rights reserved.

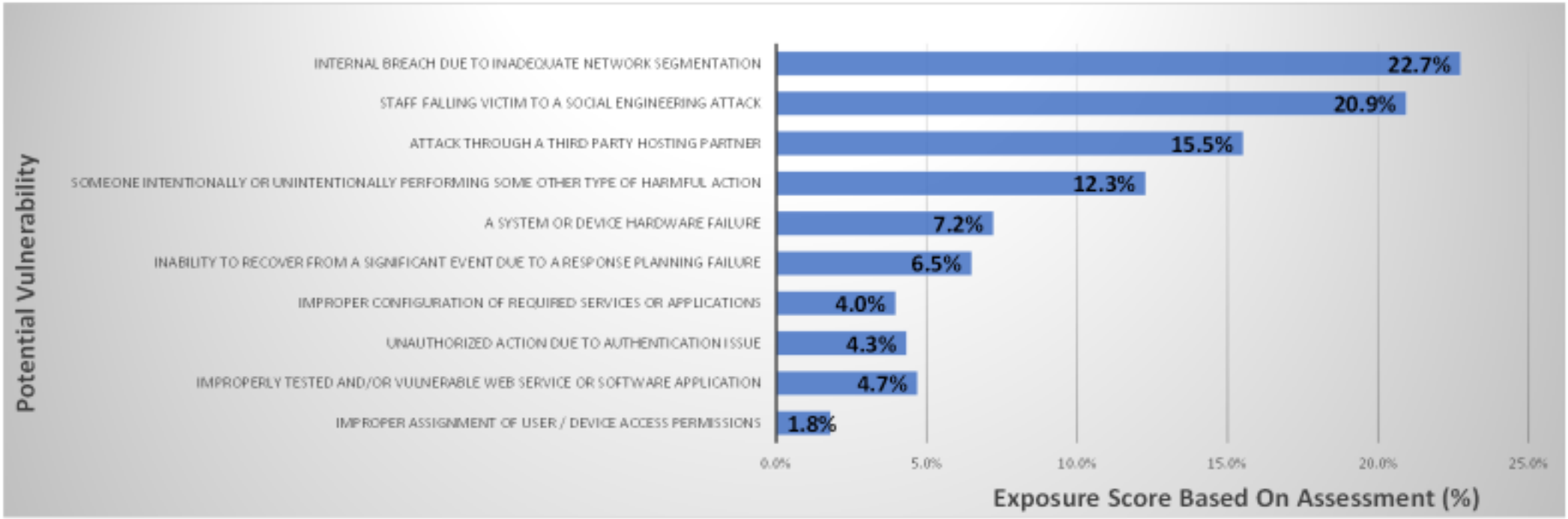
© 2024 SVAM. All Rights Reserved.

Matrix			Potential Events						
			Confidentiality	Integrity	Availability				Compliance
			Confidential/Sensitive data is disclosed	Confidential/Sensitive data is improperly modified	Confidential/Sensitive data is unavailable or lost	Access to critical asset is unavailable or lost	Insufficient staff are available to perform critical duties	Disruption of supplies	Non-compliance (Education Law 2D & CIPA) causes significant financial or operational impact
Potential Vulnerabilities	People	Attack through a third party hosting partner	3	3				3	3
		Staff falling victim to a social engineering attack	3	3	3	3			3
		Improper assignment of user / device access permissions							
		Someone intentionally or unintentionally performing some other type of harmful action	3	3	3	3			
		System or staff unavailability due to capacity issue							
	Process	Poor practices due to lack of effective policy							
		Unauthorized physical access to restricted location							
		Improper configuration of required services or applications							
		Inability to recover from a significant event due to a response planning failure				3			
	Technology	Internal breach due to inadequate network segmentation	3	3	3	3		3	3
		Improperly tested and/or vulnerable web service or software application	3						
		Unauthorized action due to authentication issue							3
		A system or device hardware failure				3			

© 2024 SVAM. All Rights Reserved.

Risk Profiling Assessment: Results of Vulnerability Scoring

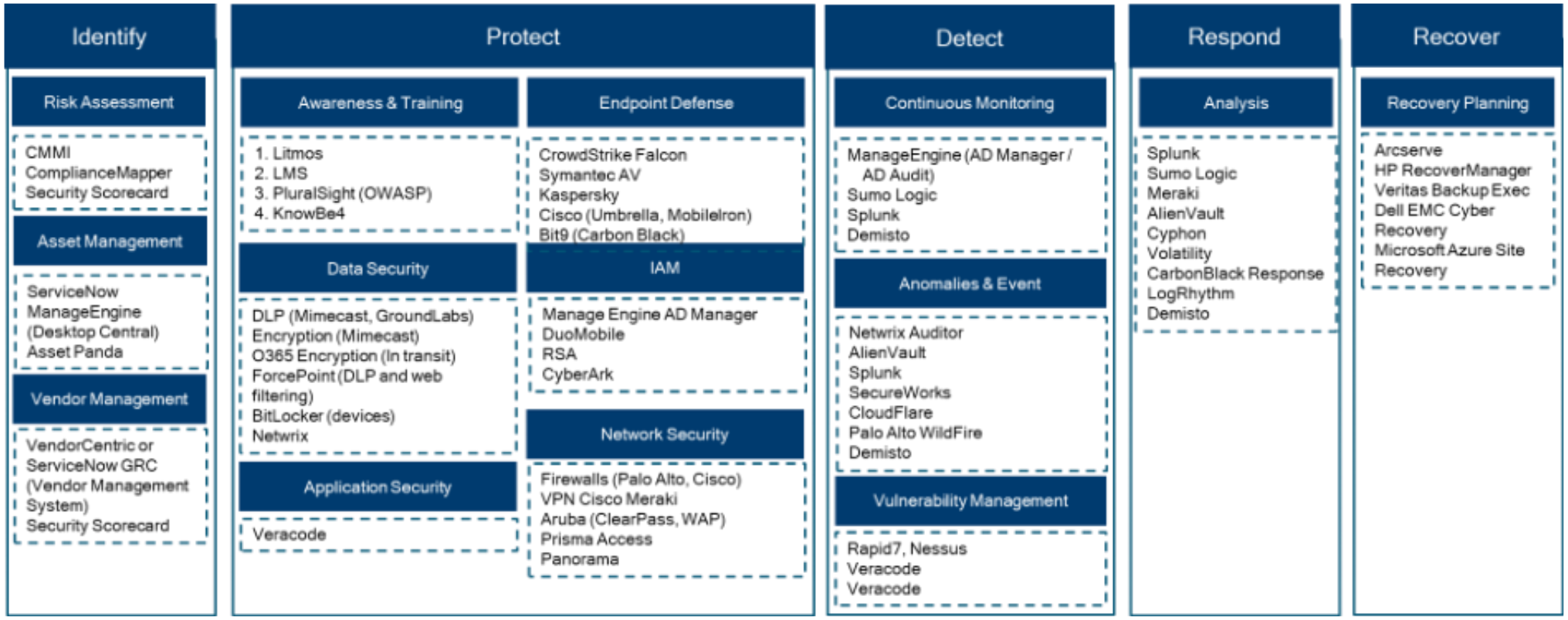
This section shows the breakdown of top potential vulnerabilities and the relative exposure for cyber-attack scenarios based on the responses from each vertical regardless of the current maturity state of related controls. The results depicted below are based on a weighted score (see Appendix).



©2022 SVAM International Inc proprietary, confidential. All rights reserved.

© 2024 SVAM. All Rights Reserved.

ILLUSTRATION OF TOOL ALIGNMENT WITH NIST CSF



©2021 SVAM International Inc proprietary, confidential. All rights reserved.

© 2024 SVAM. All Rights Reserved.

Net Message

- The organization hosts critical applications that process sensitive personal information. Therefore, with known evolving cybersecurity threat landscape, the department is increasingly at the risk of cyber attacks
- "Tone at the Top", management's leadership, and attention to cybersecurity risk management program is currently providing the opportunity for the CISO organization to identify areas for improvement and develop a roadmap to align with business objectives
- Given the limited budget and resources in the past, the organization's Cybersecurity program has done a good job maintaining the confidentiality, integrity, and availability of systems and data. However, this is not sustainable and requires continuous management's attention, sponsorship, and support
- In keeping pace with evolving threats, the organization must increase focus on enhancing their cybersecurity and data privacy controls in alignment with ongoing technology refresh and planned retirement of legacy systems. Security controls must be embedded in the application development, infrastructure, and other IT solution deployments
- Various components of organization's Cybersecurity Risk Management program are highlighted to be enhanced, including but not limited to governance and resources, effective alignment and enforcement of policies, third-party risk management, vulnerability management, threat intelligence, data protection, identity and access management, and secure software development standards and processes
- Through Management's commitment, significant investments to source additional resources using a phased approach is required to enable implementation and execution of recommended program enhancements
- Given the recommended roadmap and planned implementations across various cybersecurity functions, a centrally managed program governance is required to effectively manage all activities, both within the program and all other projects with dependencies to cybersecurity control functions
- The organization's robust Information Security policies and procedures must be developed and fully executed to align with required compliance and laws and establish baseline for all implementation projects and on-going practices. On an annual basis an independent assessment and audit of program improvements and effectiveness is highly recommended

©2021 SVAM International Inc proprietary, confidential. All rights reserved.

© 2024 SVAM. All Rights Reserved.

SVAM INTERNATIONAL, INC.

EDUCATION USE CASE



How SVAM helped the New York City Department of Education design and implement a Cybersecurity Program

Challenge:

DOE holds data for over 1.2 million students and 150,000 employees and uses around 600 applications; the critical applications can access the PII of a large number of end users - with few critical applications still using the legacy infrastructure. Limited governance program and enforcement of corporate cybersecurity requirements; lack of security and awareness and training program. Many of DOE's applications are implemented with the help of Third-party vendors; processes were not established to sufficiently assess and manage vendor risks, leading to Supply chain risk. Absence of an established SOC; shortages of IT staff, including cybersecurity resources

Solution:

Establish a Third-Party Risk Management program through the initiation of a vendor inventory, risk rating, and governance, thereby establishing Third-Party annual due diligence, issue tracking process, and corrective action Operationalize governance policies to ensure timely adoption of the enhanced processes and implement the proposed organizational structure using a phased approach. Develop SOC strategy and framework in alignment with city-wide policies set forth by NYCC. Implement processes related to newly developed IR plan and track its adoption; execute table-top exercises for critical scenarios. Establish a formal enterprise-wide IR Plan to identify, analyze, contain, eradicate, and recover from incidents and testing activities.

Outcomes:

12 → 2

Reduction of vendor assessment cycle times in weeks.

75%

Enhanced vendor risk metrics after implementing an automated alerting system.

© 2024 SVAM. All Rights Reserved.

SVAM INTERNATIONAL, INC.

State, Local and Education Clients



SLED CLIENTS

© 2024 SVAM. All Rights Reserved.

SVAM
INTERNATIONAL, INC.

SVAM CYBERSECURITY LEADERSHIP



Anil Kapoor
President & CEO

anil@svam.com
Anil Kapoor (LinkedIn)



Vikas Dhablania
Chief Operating Officer

vikas@svam.com
Vikas Dhablania (LinkedIn)

Partners with Purpose

Driving meaningful change through digital acceleration.

Public Sector Cybersecurity Leadership

Scott Mastellon
Public Sector



LinkedIn Profile

Kiran Bhujle
Cybersecurity



LinkedIn Profile

Matt Lang
Cybersecurity



LinkedIn Profile

Kambiz Mofrad
Cybersecurity



LinkedIn Profile

Shahryar Shaghaghi
Cybersecurity



LinkedIn Profile

© 2024 SVAM. All Rights Reserved.

Primary Contact for Nassau County School Districts

PRIMARY SVAM CONTACT

Scott Mastellon, Managing Director, Public Sector



Office: 516-320-8693
smastellon@svam.com
233 E Shore Rd, Suite 201,
Great Neck, NY 11023

© 2024 SVAM. All Rights Reserved.