ncx group

Secure24 Comprehensive Security Review

Prepared for:

Grossmont-Cuyamaca Community College District

Table of Contents

EXECUTIVE SUMMARY

NCX is pleased to be able to provide the following security assessment results.

Security Program Background

A quick review of some of the cybersecurity breaches from 2018 shows us why having a security program is so vital.

The University at Buffalo suffered a data breach of external third-party accounts which has affected more than 2,500 accounts campus-wide. About 1,800 of those are student accounts.

The University of Alaska suffered a data breach of over fifty accounts of current and former employees and students.

Palo Alto Unified School District learned an employee was storing confidential parent information on his laptop. The District's investigation determined that although the stolen laptop was password protected, confidential information may have been stored on the device, including the names, addresses, and Social Security numbers of several residents.

Thomas Edison State University discovered that an unauthorized user accessed a Thomas Edison employee's email account. Thomas Edison reasonably believes that the Unauthorized User improperly acquired the personal information of 557 individuals.

No matter how large or small your company is, you need to have a plan to ensure the security of your information asset. Your security program makes you think holistically about your organization’s security. The security program provides the framework for keeping your company at the desired security level by assessing the risks you face, deciding how you will mitigate them, and planning for how you maintain the program and your security practices up to date.

A security program is vital because it helps you maintain your focus on IT security and enables you to identify and stay in compliance with the regulations that affect how you manage your data. It keeps you on the right footing with your clients and your customers so that you meet both your legal and contractual obligations. Its life cycle process ensures that security is continuously adapting to your organization and today's ever-changing IT environment.

One of the most significant obstacles facing organizations today is complexity. Cybersecurity involves the merging of regulatory requirements, the fusion of internally and externally based threats. It requires a plan to manage this in an ecosystem of diverse technologies managed by multiple areas of an organization. It’s just a massive pool of complexity. This complexity includes mobile devices, network devices, applications, infrastructure, cloud-based systems and software service products, third-party vendor

relationships and it all piles into the security program. The goal is how do you separate that into manageable pieces so you can effectively manage risk? And, how do you prioritize inside that broad portfolio and make sure you're focusing on things at the right time?

Because all the publicity goes to the massive breaches, external threats have the podium right now and you have to pay attention to that. At the same time, you have to keep your eye on the ball with internal threats. The probability of an internal threat is more significant than an external threat. You have a trusted environment where you've done background investigations of people accessing your system, and you trust them, and for the most part, they are doing good things, but occasionally you do have a situation where somebody does things inappropriately internally inside your network, and you have to take action.

Benefits of a well-defined security program

A clearly defined security program provides the best framework for complying with information security legal, regulatory and contractual requirements. The program also proves that senior management is committed to the security of the organization, including the customer's information. The security program allows you to be focused on reducing the risks of information that is valuable for the organization, which in turn provides a common goal for the company. Your security program also helps to optimize operations within the organization because of clearly defined responsibilities and business processes. The end goal is it provides the ability to build a culture of security.

SCOPE OF PROJECT

The scope of this project included a full review of the organization's security program. To

use the Cybersecurity Framework from the National Institute of Standards and Technology (NIST), the following areas were reviewed (the titles in () refer to the section in the report where this is covered in detail:

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Asset Management	**Access Control**	**Anomalies and Events** (Incident Response)	**Response Planning** (Incident Security Management)	**Recovery Planning** (Business Continuity Management)
Business Environment (Compliance)	**Awareness & Training** (Human Resource Security)	**Security Continuous Monitoring** (Communication & Operations Management)	**Communications** (Communication & Operations Management)	**Improvements** (Incident Security Management)
Governance (Organization of Information Systems)	**Data Security** (Physical & Environmental Security)	**Detection Processes** (Communication & Operations Management)	**Analysis** (Incident Security Management)	**Communications** (Incident Security Management)
Risk Assessment (Asset Management)	**Information Protection Processes & Procedures** (Security Policy)		**Mitigation** (System Vulnerabilities)	
Risk Management Strategy (Security Policy)	**Maintenance** (System Vulnerabilities)		**Improvements** (Incident Security Management)	
	Protective Technology (IS Acquisition, Development, and Maintenance)			

Identify - Cybersecurity practices that provide the foundation for how the business aligns with cybersecurity. *Example: A cybersecurity governance program containing the policies and procedures allowing the organization to maintain adherence to legal and regulatory requirements.*
Protect - Controls and safeguards to protect or deter a cybersecurity threat from materializing. *Example: Data at rest, in motion, and in use is protected.*

Detect - Continuous monitoring to provide proactive and real-time alerting of cybersecurity-related events. *Example: Detection processes and procedures which includes periodic testing to validate awareness of unusual incidents.*

Respond - Response activities which are executed during a cybersecurity incident. *Example: Incident Response Program and root cause analysis.*

Recover - Business continuity plans to recover services impacted by a cyber breach. *Example: Disaster recovery simulation exercises and redundant operations.*

SECURITY PROGRAM MATURITY SCORE

Each of these areas is scored on a scale of 1-5

SCORE	DESCRIPTION
1 – Nonexistent	Lack of policies, procedures, or process in place resulting in employees having no concept of the threat.
2 – Compliance Focused	Policies are in place that are designed to help meet compliance objectives. Employees have limited training and are unsure about standard policy.
3 – Promoting awareness & behavior change	Annual training and continual reinforcement occurs. Awareness of threats exists and changes in employee behavior to actively recognize, prevent, and report incidents occur.
4 – Long-term sustainment & culture change	A continuous training program exists and good cybersecurity behavior embedded within the corporate culture.
5 – Metrics framework	Metrics are in place to demonstrate a programs progress, improvement, and impact.

AREA	DESCRIPTION	SCORE

Identify	The ability to manage cybersecurity risks to systems, assets, data, and other business capabilities.	1
Protect	Capacity to develop and integrate the appropriate safeguards to facilitate the function of the business.	1
Detect	The ability to identify the occurrence of a cybersecurity event.	2
Respond	Capacity to enforce timely response to a detected cybersecurity event.	1
Recover	The ability to take appropriate actions to restore systems and assets after a cybersecurity event.	2
	OVERALL MATURITY SCORE	7

NEXT STEPS

NCX recommends these as the top priorities for Grossmont-Cuyamaca Community College District:

- **Develop a comprehensive security policy** – this will provide the framework to develop the entire security program. By prioritizing the security policy, it will provide a basis for process, product, and project development and decisions.
- **Implement a central log collection server** – this will allow the District to have logs in the event of a security event without the concern about the volume of traffic.
- **Create a position focused on cybersecurity** – The cybersecurity landscape is dynamic and needs someone who has a focus on remaining current and helps drive projects to ensure the security posture of the District remains strong. A short-term stop-gap measure would be to have someone on the current staff have at least 30% of their job be focused on cybersecurity.

APPENDIX A: REMEDIATION MATRIX

The following matrix has been developed to help guide a remediation effort for the findings in this report:

AREA	DESCRIPTION	PRIORITY	OWNER
Business Continuity	Create a business continuity plan	High	
Communication & Operations	Create a required separation of duties for firewall rule changes	High	
Communication & Operations	Implement a central log collection server	High	
Human Resource	Create a social media policy	High	
Incident Security	Create a forensic response plan	High	
Incident Security	Create an incident security response plan	High	
Security Policy	Create a comprehensive security policy	High	
Security Policy	Create comprehensive security policy	High	
System Vulnerabilities	Apply Oracle patches	High	
System Vulnerabilities	Change SNMP strings to be complex and follow the same guidelines as passwords	High	
System Vulnerabilities	Disable rexec service	High	
System Vulnerabilities	Disable rlogin service	High	
System Vulnerabilities	Replace default IIS Welcome Page with relevant Content	High	
System Vulnerabilities	Require clients to use TLS version 1.2	High	
System Vulnerabilities	Set password for the listener control service for Oracle	High	
System Vulnerabilities	Update all Microsoft software	High	
System Vulnerabilities	Upgrade HP Data Protector Version	High	
System Vulnerabilities	Upgrade obsolete Microsoft SQL Server version	High	
System Vulnerabilities	Upgrade obsolete Oracle software	High	
System Vulnerabilities	Upgrade OpenSSH	High	
System Vulnerabilities	Upgrade Sendmail software	High	
Access Control	Create a formal access control program	Medium	
Access Control	Create a formal structured audit program	Medium	
Access Control	Evaluate a Privileged Access Management Solution	Medium	

AREA	DESCRIPTION	PRIORITY	OWNER
Access Control	Evaluate Privileged Account Management solutions	Medium	
Access Control	Evaluate strengthening mobile device controls	Medium	
Asset Management	Create a specific asset management process and policy	Medium	
Asset Management	Create information classification guidelines	Medium	
Communication & Operations	Create a formal change control policy	Medium	
Communication & Operations	Create a formal firewall policy review process and procedure	Medium	
Communication & Operations	Create a formal system acceptance process and procedure	Medium	
Communication & Operations	Create system documentation for key systems	Medium	
Communication & Operations	Evaluate monitoring systems for the District network	Medium	
Communication & Operations	Evaluate NAC solutions	Medium	
Human Resource	Create a formal security awareness training program	Medium	
Human Resource	Create security awareness training metrics	Medium	
IS Acquisition	Create a formal process for software acquisition	Medium	
IS Acquisition	Run regular vulnerability checks	Medium	
Organization of Information Systems	Create a position focused on cybersecurity	Medium	
Organization of Information Systems	Increase management's commitment to cybersecurity	Medium	
System Vulnerabilities	Disable HTTP DELETE Method	Medium	
System Vulnerabilities	Disable HTTP TRACE Method	Medium	
System Vulnerabilities	Disable NULL sessions	Medium	
System Vulnerabilities	Disable SSLv2 protocol support	Medium	
System Vulnerabilities	Disable support for 3DES suite	Medium	
System Vulnerabilities	Disable support for DES and IDEA cipher suites.	Medium	
System Vulnerabilities	Disable support for RC4 ciphers.	Medium	

AREA	DESCRIPTION	PRIORITY	OWNER
System Vulnerabilities	Disable the EXPN and VRFY commands on your SMTP server.	Medium	
System Vulnerabilities	Disable the telnet service. Replace it with technologies such as SSH, VPN, or TLS.	Medium	
System Vulnerabilities	Enable HTTPS on the Web server.	Medium	
System Vulnerabilities	Replace expired SSL Certificates	Medium	
System Vulnerabilities	Replace the default Welcome page on IIS servers with relevant content	Medium	
System Vulnerabilities	Require clients to use TLS version 1.2 using Authenticated Encryption with Associated Data (AEAD) capable ciphers.	Medium	
System Vulnerabilities	Require clients to use TLS version 1.2 using Authenticated Encryption with Associated Data (AEAD) capable ciphers.	Medium	
System Vulnerabilities	Restrict the processing of DNS queries to only systems that should be allowed to use this nameserver.	Medium	
System Vulnerabilities	Restrict the processing of recursive queries to only systems that should be allowed to use this nameserver.	Medium	
System Vulnerabilities	Upgrade Apache HTTPD	Medium	
System Vulnerabilities	Upgrade OpenSSL	Medium	
System Vulnerabilities	Use 2048-bit or stronger Diffie-Hellman groups with safe primes	Medium	