State of North Dakota
Security Assessment Report

[2021 Executive Summary]
[SANITIZED VERSION]

SECUREYETI

DOCUMENT REVISION HISTORY

VERSION	DATE	CHANGE DESCRIPTION
1.0	01/31/2021	Initial Draft
1.1	02/17.2021	Added Responses
-	-	-

SUBMITTED TO:

Cory Walcker
Information Technology Auditor
Office of the State Auditor

(701) 328-2512
cwalcker@nd.gov

PREPARED BY:

Brett Lessley
Project Manager
Secure Yeti

(918) 986-7060
brett.lessley@secureyeti.com

TABLE OF CONTENTS

1. INTRODUCTION

Under the guidance and direction of the State Auditor's office, Secure Yeti conducted a network security assessment of key network resources and infrastructure utilized by North Dakota's State Agencies and the state-funded North Dakota University System (NDUS).

The objective of this assessment was to evaluate the overall security posture of the network by subjecting network systems and resources to methods and techniques commonly used by hackers and malicious actors. This process allows for the proactive remediation of any identified weakness or vulnerability before they can be exploited by a hacker to gain unauthorized access to critical systems or sensitive data.

From 10/01/2020 through 01/31/2021, Secure Yeti performed a vulnerability assessment and penetration test against the internal and external networks of thirteen separate state-funded entities. Additional on-site wireless (WiFi) and physical tests were also conducted at six of the thirteen locations. All involved entities were also subjected to a custom-built phishing campaign.

It is important to note that this report represents a "snapshot" of each environment at the particular point-in-time that it was assessed. The security posture observed during testing may have improved, deteriorated or remained the same since this assessment was completed.

Secure Yeti understands the importance that the State of North Dakota has placed on IT security. We sincerely appreciate the opportunity to have worked with the State Auditor's Office during this engagement. Should you have any questions regarding these findings, or the content of this report, please feel free to contact us.

2. KEY PARTICIPANTS

OFFICE OF THE STATE AUDITOR

Josh Gallion State Auditor	jcgallion@nd.gov (701) 328-4780
Cory Walcker Information Technology Auditor	cwalcker@nd.gov (701) 328-2512

INFORMATION TECHNOLOGY DEPARTMENT (ITD)

Uriah Burchinal Governance & Risk Compliance Manager	uburchinal@nd.gov (701) 328-2164

NORTH DAKOTA UNIVERSITY SYSTEM (NDUS)

Darin King Vice Chancellor IT / CIO	darin.r.king@ndus.edu (701) 777-4237
Brad Miller Director of Information Security	brad.miller@ndus.edu (701) 777-3587
Bryan Ford Senior Security Engineer	bryan.ford@ndus.edu (701) 777-6484
Michael Roue Security Apprentice	michael.roue@ndus.edu (701) 777- 3402

SECURE YETI

Brett Lessley Project Manager	brett.lessley@secureyeti.com (918) 986-7060 x1005
Casey Bourbonnais Lead Technical Tester	casey.bourbonnais@secureyeti.com (918) 986-7060 x1010

3. SUMMARY OF SCOPE

The scope included the assessment of network resources at thirteen state-funded entities.

(ITD)	Information Technology Department
(CTS)	Core Technology Services
(BSC)	Bismarck State College
(DCB)	Dakota College at Bottineau
(DSU)	Dickinson State University
(LRSC)	Lake Region State College
(MaSU)	Mayville State University
(MiSU)	Minot State University
(NDSCS)	North Dakota State College of Science
(NDSU)	North Dakota State University
(UND)	University of North Dakota
(VCSU)	Valley City State University
(WSC)	Williston State College

Specific IP ranges and subnets were defined in advance for each location before the assessment began.

Resources were evaluated using three separate angles of attack:

- External User with no access to network resources provided. This approach evaluates risk from the perspective of a hacker.
- Internal User with no access to network resources provided. This approach evaluates risk from the perspective of a visitor.
- Internal User with network access given to a typical employee. This approach evaluates risk from the perspective of a malicious insider or disgruntled employee.

External testing was conducted from eight different locations. ITD and NDUS whitelisted Secure Yeti's external IP addresses so they wouldn't be blocked.

Internal Testing was performed using remote testing units supplied by Secure Yeti. These units were deployed to the same network subnets that hosted standard employee workstations at each location.

TOTAL IP ADDRESSES: 565,180

EXTERNAL ADDRESSES: 94,000

INTERNAL ADDRESSES: 466,560

EXCLULSIONS: 4,620

CIDR BLOCK	BLOCK SIZE (IN IP's)	BLOCKS	TOTAL
/15	131,072	1	131,072
/16	65,536	4	262,144
/18	16,384	3	49,152
/19	8,192	1	8,192
/20	4,096	7	28,672
/21	2,048	4	8,192
/22	1,024	12	12,288
/23	512	35	17,920
/24	256	183	46,848
/25	128	5	640
/27	32	1	32
/28	16	1	16
/32	1	12	12

(*SUMMARY OF THE IP SPACE AND UNIQUE CIDR BLOCKS TESTED.)*

4. EXCLUSIONS

The following exclusions were agreed upon at the beginning of the assessment.

- Network segments supporting critical Public Safety infrastructure and the 911 system were out of scope and not tested.
- Network segments supporting the State Election System were out of scope and not tested.
- Network segments supporting the State Penitentiary System were out of scope and not tested.
- Denial of Service (DoS) attacks were not included in the testing methodology and were not intentionally initiated or attempted.
- All storage arrays and supporting infrastructure were considered out of scope for intrusive testing. This includes SAN, NAS, iSCSI arrays, in addition to fibre-channel or iSCSI controllers and switches.

5. METHODOLOGY

Vulnerability Assessment: used automated tools to systematically review/scan network resources for known security weaknesses and misconfigurations.

ITD	CTS	BSC	DCB	DSU	LRCS	MaSU	MiSU	NDSCS	NDSU	UND	VCSU	WSU
X	X	X	X	X	X	X	X	X	X	X	X	X

Penetration Testing: attempted to exploit discovered weaknesses and vulnerabilities to gain unauthorized access to network resources.

ITD	CTS	BSC	DCB	DSU	LRCS	MaSU	MiSU	NDSCS	NDSU	UND	VCSU	WSU
X	X	X	X	X	X	X	X	X	X	X	X	X

Phishing Campaign: sent fake emails to employees in an attempt to trick them into divulging credentials or clicking bogus links.

ITD	CTS	BSC	DCB	DSU	LRCS	MaSU	MiSU	NDSCS	NDSU	UND	VCSU	WSU
X	X	X	X	X	X	X	X	X	X	X	X	X

Wireless Network Assessment: used specialized scanners to detect misconfigurations in the wireless network setup, verified strength of wireless encryption, identified and located rogue access points, provided heat maps of wireless network coverage.

ITD	CTS	BSC	DCB	DSU	LRCS	MaSU	MiSU	NDSCS	NDSU	UND	VCSU	WSU
X	X	X	-	X	-	-	-	-	-	X	X	-

Physical Assessment: identified opportunities to compromise physical barriers protecting network resources, including sensors, cameras, door locks, exposed network ports, and unattended workstations to gain unauthorized access to secure areas.

ITD	CTS	BSC	DCB	DSU	LRCS	MaSU	MiSU	NDSCS	NDSU	UND	VCSU	WSU
X	X	X	-	X	-	-	-	-	-	-	X	-

Legend:
(ITD) Information Technology Department
(CTS) Core Technology Services
(BSC) Bismarck State College
(DCB) Dakota College at Bottineau
(DSU) Dickinson State University
(LRSC) Lake Region State College
(MaSU) Mayville State University
(MiSU) Minot State University
(NDSCS) North Dakota State College of Science
(NDSU) North Dakota State University
(UND) University of North Dakota
(VCSU) Valley City State University
(WSC) Williston State College

6. RISK RATING SYSTEM

Critical *(16-POINTS)*	Critical severity ranking requires immediate action through mitigating controls, direct remediation or a combination thereof. Exploitation of discovered critical severity vulnerabilities not only results in privileged access to the target system/application and/or sensitive data but also allows access to other hosts or data stores within the environment.
High *(8-POINTS)*	A finding denoted with a high severity ranking suggests that this observation requires immediate evaluation and subsequent resolution. Exploitation of high severity vulnerabilities discovered in the environment can lead directly to an attacker gaining privileged access (e.g. administrator, root, SA, etc.) to the system/application and/or sensitive data.
Medium *(4-POINTS)*	A finding denoted with a medium severity ranking requires review and resolution within a short period. From a technical perspective, vulnerabilities that warrant a medium severity ranking can lead directly to an attacker gaining non-privileged access (e.g. standard user) to the system/application and/or sensitive data or cause a denial-of-service (DoS) condition on the host, service or application.
Low *(2-POINTS)*	A finding denoted with a low severity ranking requires an evaluation for review and resolution once the remediation efforts for critical, high and medium severity issues are complete. From a technical perspective, vulnerabilities that warrant a low severity ranking may leak information to unauthorized or anonymous users used to launch a more targeted attack against the environment.
Info *(1-POINT)*	An informational notation presents no direct threat to the confidentiality, integrity or availability of the data or systems supporting the environment. These issues pose an inherently low threat to the organization and any proposed resolution should be considered as an addition to the information security procedures already in place.

7. CONTROL FAMILIES / RISK CATEGORIES

CONTROL FAMILY		DESCRIPTION
Access Control	(AC)	The AC Control Family consists of security requirements detailing who has access to what assets and reporting capabilities like account management, system privileges, and remote access logging to determine when users have access to the system and their level of access.
Audit & Accountability	(AU)	The AU control family consists of security controls related to an organization's audit capabilities. This includes audit policies and procedures, audit logging, audit report generation, and protection of audit information.
Awareness & Training	(AT)	The control sets in the AT Control Family are specific to your security training and procedures, including security training records.
Configuration Management	(CM)	CM controls are specific to an organization's configuration management policies. This includes a baseline configuration to operate as the basis for future builds or changes to information systems. Additionally, this includes information system component inventories and a security impact analysis control.
Contingency Planning	(CP)	The CP control family includes controls specific to an organization's contingency plan if a cybersecurity event should occur. This includes controls like contingency plan testing, updating, training, and backups, and system reconstitution.
Identification & Authentication	(IA)	IA controls are specific to the identification and authentication policies in an organization. This includes the identification and authentication of organizational and non-organizational users and how the management of those systems.
Incident Response	(IR)	IR controls are specific to an organization's incident response policies and procedures. This includes incident response training, testing, monitoring, reporting, and response plan.
Maintenance	(MA)	The MA controls in NIST 800-53 revision five detail requirements for maintaining organizational systems and the tools used.
Media Protection	(MP)	The MP family includes controls that are specific to access, marking, storage, transport policies, sanitization, and defined organizational media use.
Personnel Security	(PS)	PS controls relate to how an organization protects its personnel through position risk, personnel screening, termination, transfers, sanctions, and access agreements.
Physical & Environmental Protection	(PE)	The PE control family is implemented to protect systems, buildings, and related supporting infrastructure against physical threats. These controls include physical access authorizations, monitoring, visitor records, emergency shutoff, power, lighting, fire protection, and water damage protection.

CONTROL FAMILY		DESCRIPTION
Planning	(PL)	PL controls in NIST 800-53 are specific to an organization's security planning policies and must address the purpose, scope, roles, responsibilities, management commitment, coordination among entities, and organizational compliance.
Program Management	(PM)	The PM control family is specific to who manages your cybersecurity program and how it operates. This includes, but is not limited to, a critical infrastructure plan, information security program plan, plan of action milestones and processes, risk management strategy, and enterprise architecture.
Risk Assessment	(RA)	The RA control family relates to an organization's risk assessment policies and vulnerability scanning capabilities.
Security Assessment & Authorization	(CA)	The CA control family includes controls that supplement the execution of security assessments, authorizations, continuous monitoring, plan of actions and milestones, and system interconnections.
System & Communications Protection	(SC)	The SC control family is responsible for systems and communications protection procedures. This includes boundary protection, protection of information at rest, collaborative computing devices, cryptographic protection, denial of service protection, and many others.
System & Information Integrity	(SI)	The SI control family covers controls that protect system and information integrity. These include flaw remediation, malicious code protection, information system monitoring, security alerts, software and firmware integrity, and spam protection.
System and Services Acquisition	(SA)	The SA control family relates to controls that protect allocated resources and an organization's system development life cycle. This includes information system documentation controls, development configuration management controls, and developer security testing and evaluation controls.

8. EXECUTIVE SUMMARY

8.1. RISK ASSIGNMENT

Testing discovered a total of 128 unique findings across the 13 entities being assessed. After a thorough analysis, these findings have been rated at the following risk levels:

RISK LEVEL:	COUNT:
CRITICAL	5
HIGH	57
MEDIUM	33
LOW	33
INFO	0
TOTAL:	**128**

In determining risk, our team analyzed two key factors for each finding:

1) IMPACT: defined as "the magnitude of harm that can be expected". When calculating impact, the following possibilities are considered:

- degradation of mission capabilities
- damage / loss of organizational assets or data (& sensitivity of that data)
- financial loss
- reputational loss
- loss of life or physical harm

2) LIKELIHOOD: definded as "the probablilty of an event occuring". When calculating likelihood, we consider:

- the likelihood of the event occurring or being initiated
- the likelihood of the event being successful
- factors that mitigate risk (i.e. – small user-base, located on an isolated network, rarely used)
- factors that magnify risk (i.e. – publically accessible, weak password policies, misconfigurations)

LIKELIHOOD \ IMPACT	Info	Low	Medium	High	Critical
Critical	Info	Low	Medium	High	Critical
High	Info	Low	Medium	High	Critical
Medium	Info	Low	Medium	Medium	High
Low	Info	Low	Low	Low	Medium
Info	Info	Info	Info	Low	Low

OVERALL RISK

OVERALL RISK DETERMINATION CHART – BASED ON IMPACT-LIKELIHOOD ANALYSIS.

8.2. CONTROL FAMILY CATEGORIZATION

In addition to the assessment of risk, each finding is also sorted into functional categories, also known as “control families”.

If the observed deficicency for a particular finding applies to multiple families, a secondary classification is assigned.

The table below shows the breakdown of findings based on control families:

CONTROL FAMILIES:	PRIMARY	SECONDARY	TOTAL
Access Control	31	24	55
Audit & Accountability	0	0	0
Awareness & Training	11	0	11
Configuration Management	18	19	37
Contingency Planning	0	1	1
Identification & Authentication	17	2	19
Incident Response	2	0	2
Maintenance	0	0	0
Media Protection	4	0	4
Personnel Security	0	0	0
Physical & Environmental Protection	7	0	7
Planning	0	0	0
Program Management	0	0	0
Risk Assessment	0	0	0
Security Assessment & Authorization	0	0	0
System & Communications Protection	15	0	15
System & Information Integrity	23	0	23
System & Services Acquisition	0	0	0
TOTAL:	128	46	**174**

8.3. HEAT MAP (CONTROL FAMILY/RISK)

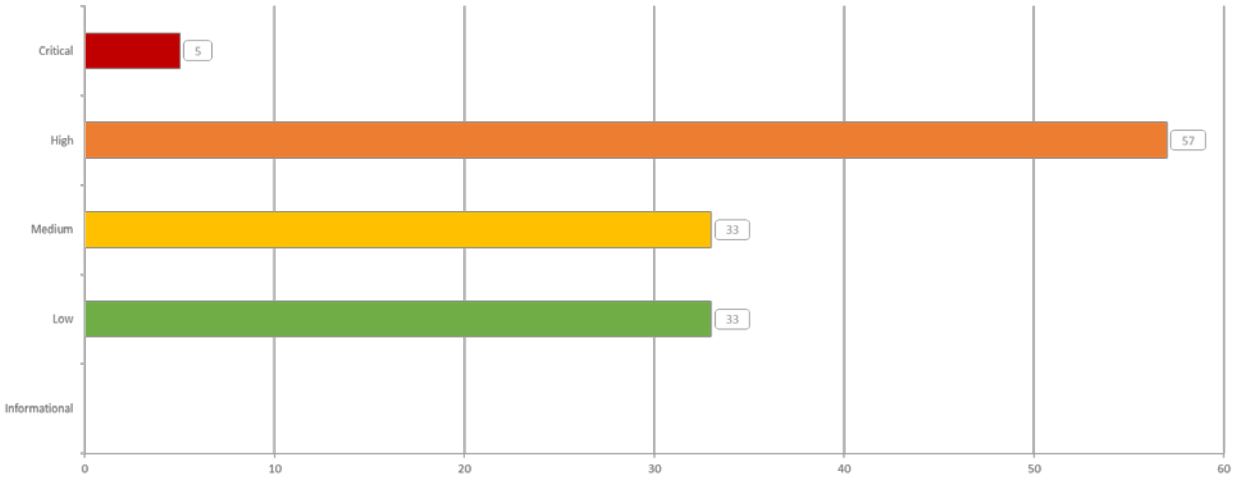
Below is a heat map that displays the number of findings for each control family, grouped by their associated level of risk.

By cross-referencing or weighting this data, we can see which areas are most problematic:

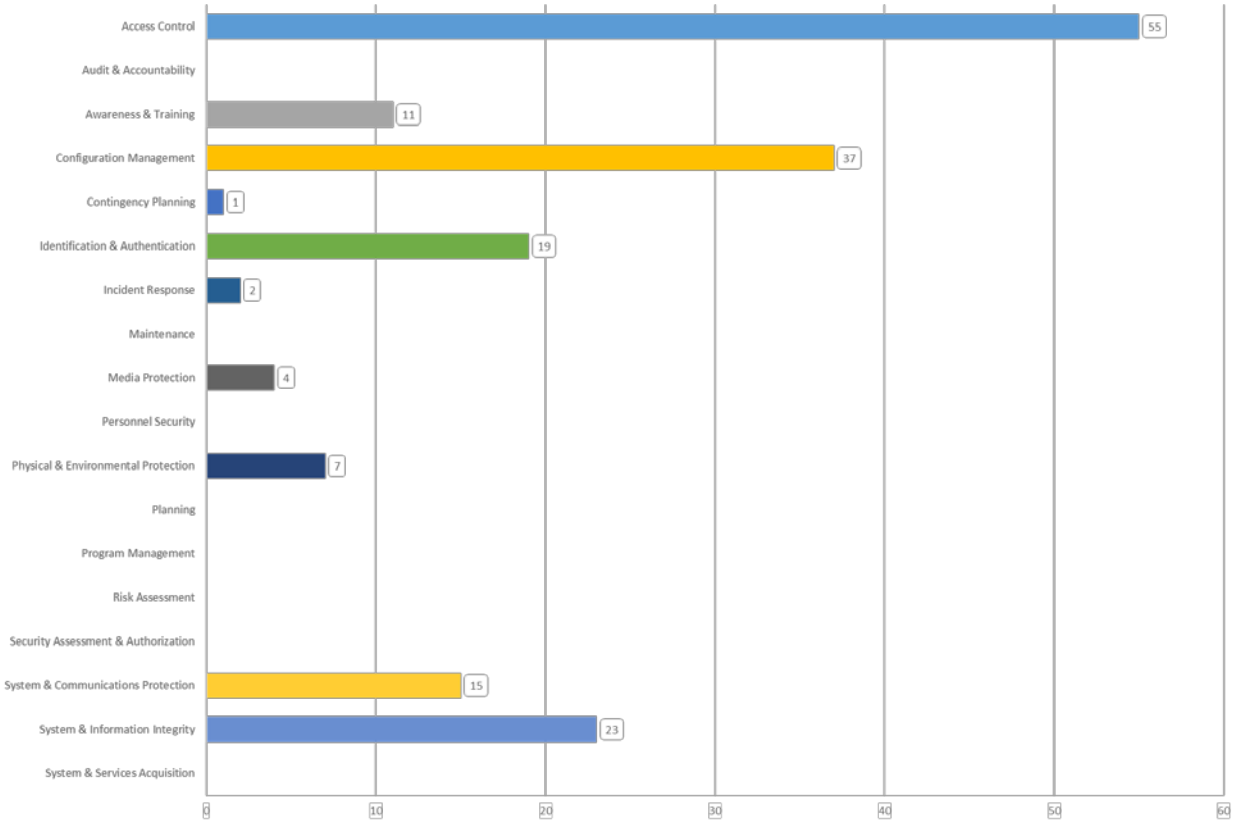
CONTROL FAMILY / RISK LEVEL:	CRITICAL (16 PTS)	HIGH (8 PTS)	MEDIUM (4 PTS)	LOW (2 PTS)	INFO (1 PNT)	TOTAL POINTS
Access Control:	1	20	22	12	0	288
Configuration Management:	0	16	7	14	0	184
System & Information Integrity:	0	12	3	8	0	124
Identification & Authentication:	0	6	8	5	0	90
System & Communications Protection:	0	7	2	6	0	76
Awareness & Training:	0	4	4	3	0	54
Media Protection:	2	1	1	0	0	44
Physical & Environmental Protection:	0	4	2	1	0	42
Incident Response:	2	0	0	0	0	32
Contingency Planning:	0	1	0	0	0	8
Audit & Accountability:	0	0	0	0	0	0
Maintenance:	0	0	0	0	0	0
Personnel Security:	0	0	0	0	0	0
Planning:	0	0	0	0	0	0
Program Management:	0	0	0	0	0	0
Risk Assessment:	0	0	0	0	0	0
Security Assessment & Authorization:	0	0	0	0	0	0
System & Services Acquisition:	0	0	0	0	0	0
TOTAL POINTS:	80	568	196	98	0	942

HEAT MAP SHOWING THE DISTRIBUTION OF FINDINGS PER CONTROL FAMILY, GROUPED BY LEVEL OF RISK.

8.4. LINE GRAPHS

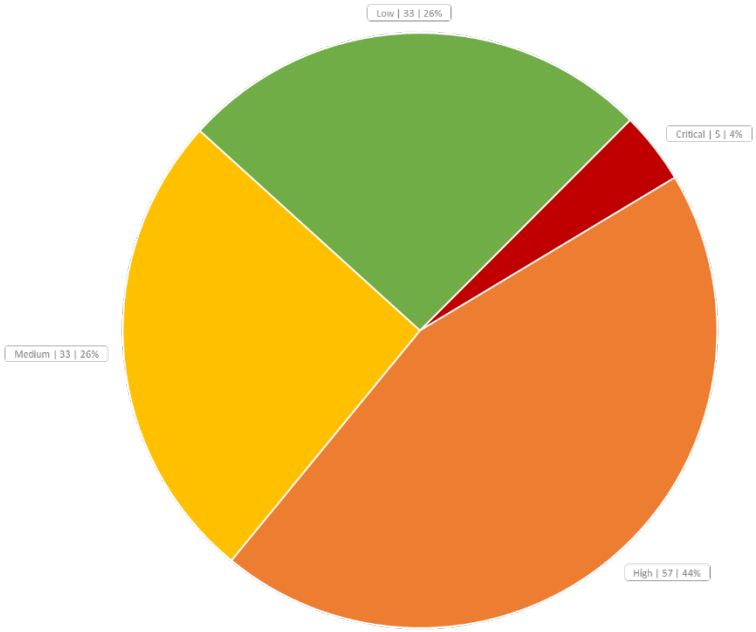


DISTRIBUTION OF FINDINGS PER RISK LEVEL

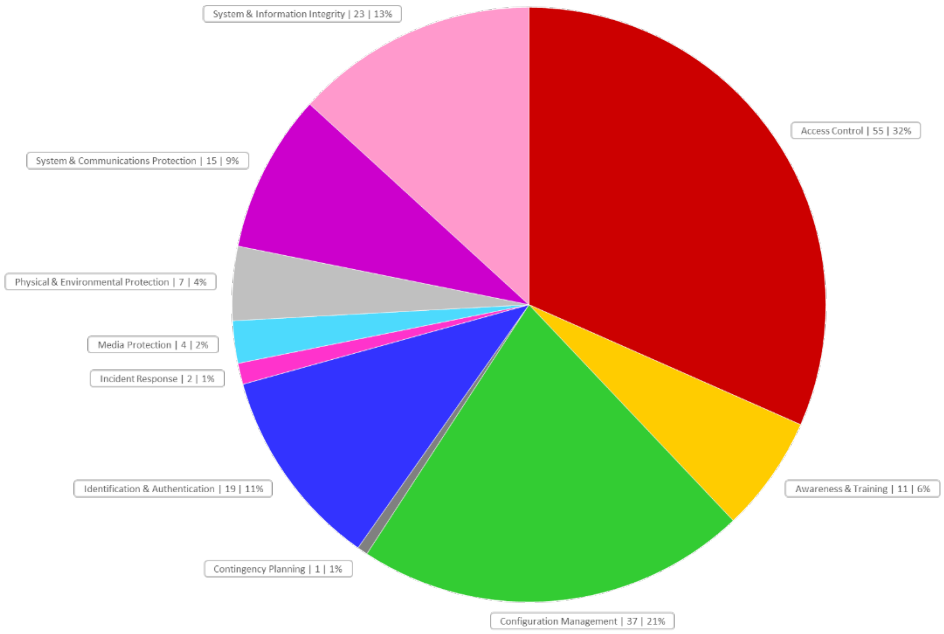


DISTRIBUTION OF FINDINGS PER CONTROL FAMILY

8.5. PIE CHARTS



PIE CHART SHOWING PERCENTAGE OF FINDINGS PER LEVEL OF RISK



PIE CHART SHOWING PERCENTAGE OF FINDINGS PER CONTROL FAMILY

8.6. KEY FINDINGS

The findings listed below represent the ten most significant issues discovered during the assessment.

These issues have wide-spread impact and pose the greatest risk to the overall environment. These findings should be given priority in any remediation efforts:

#	Finding	Risk
ES01	Intrusion Monitoring, Detection, and Response *(Category: Incident Response)*	Critical
ES02	Insecure Password Policy *(Category: Identification & Authentication + Access Control)*	High
ES03	Separate accounts not used for Privileged Activities *(Category: Access Control)*	High
ES04	Insecure Legacy Protocols *(Category: Configuration Management)*	High
ES05	Critical Datacenter Infrastructure not protected with Physical Barriers *(Category: Physical & Environmental Protection)*	High
ES06	Misconfigured Wireless Network (NDUS Guest) *(Category: Configuration Management)*	High
ES07	Unauthenticated SMTP Relay + Remote Shell = Phishing *(Category: Access Control + Identification & Authentication)*	High
ES08	Externally exposed Network Resources *(Category: System & Communication Protection + Access Control)*	High
ES09	Patching and Configuration Management *(Category: System & Information Integrity)*	Medium
ES10	STAGEnet doesn't require acknowledgement of Use Policy / Login Banner *(Category: Access Control)*	Medium

8.7. KEY FINDINGS (DETAILS)

ES01: INTRUSION MONITORING, DETECTION, & RESPONSE

What we observed:	Many activities/actions performed during penetration testing were done with the sole purpose of measuring detection and response times. Many of these activities were not detected, ignored, or had a delayed response.
What is the risk:	Today's networks are constantly under attack from hackers, malicious insiders, and even errant and unintentional actions of end-users. A successful attack is usually the culmination of a series of small events that test the configuration and rigidness of the network. Attackers will "poke and prod" the network looking for ways to obtain access until one is found. Some attacks take months to be successful, while others can occur in a matter of seconds. These events provide key indicators, and often times indisputable evidence, that a system is under attack, or has become compromised. Rapid detection and response to these indicators is a vital part of preventing attacks, or mitigating the severity and impact of successful ones.
How do we remediate:	The capability to effectively detect and respond to intrusions or security events is multifaceted. 1) An organization must have a sufficient number of qualified staff and tools dedicated to monitoring network resources on a 24/7/365 basis. 2) In addition to ability, that staff must be given the required authority to quickly respond to events as necessary. Being able to quickly isolate a potentially compromised server or workstation is vital to the protection of the overall network. 3) The full adoption and implementation of a formal Risk Management Framework along with a Continuous Monitoring plan. These frameworks dictate how projects are developed, deployed, and maintained aide detection and response efforts. It is worth noting that we realize that ITD and NDUS are at different stages of program development when it comes to Incident Response and Detection. While NDUS is perfectly positioned and the logical choice to provide a centrally managed Incident Detection and Response platform for each individual University, they currently don't have the required manpower to adequately and efficiently provide this service. ITD on the other hand, appears to have the required staff and resources to adequately monitor the network, but their efforts and responses are often delayed, sometimes by days, waiting on the authority or approval to act upon a detected incident.

ES01: NDIT RESPONSE

NDIT Response:	
Item (1):	Full adoption and implementation of a formal Risk Management Framework
Response (1):	NDIT has recently adopted the NIST Risk Management Framework (RMF) as the program for addressing risk. To date the following actions have been taken: • Information Security Officers and Risk Assessors have been formally trained in RMF • A formalized program has been developed for RMF Service Now tool implementation is on track for completion by mid-March 2021
Item (2):	NDIT has to wait on the authority or approval to act upon a detected incident
Response (2):	Due to statutory constraints, NDIT does not have the authority to act upon a detected incident without specific statutory authority or approval from the respective state entity. As a result, NDIT is continuously working with entities to build relationships that allow for security incidents to be addressed as quickly as possible. NDIT is continually exploring options as to how to improve its ability to respond to security incidents as quickly as possible. The most expedient option would be statutory authority authorizing NDIT to address security incidents as soon as they are discovered without approval from the respective state entity.

ES01: NDUS RESPONSE

NDUS Response:	
Item (1):	NDUS lacks a sufficient number of qualified staff and tools
Response (1):	Within the past several months, NDUS began an initiative to implement a Security Operations Center (SOC) with the main goal of establishing the capabilities to detect, respond to, and recover from security events. While this initiative is underway, it will still require extensive planning and a lengthy implementation. As noted in the findings, NDUS does not currently have the required manpower to adequately and efficiently provide this service, and therefore will need to identify resources to hire qualified staff members as well as fund the necessary security tools and capabilities.
Item (2):	Full adoption and implementation of a formal Risk Management Framework
Response (2):	NDUS is utilizing the National Institute of Standards and Technology (NIST) Cybersecurity Framework (NCF) and the Center for Internet Security (CIS) Critical Security Controls as the foundation for security planning and risk management.

ES02: INSECURE PASSWORD POLICY

What we observed:

Testing discovered insecure or sometimes non-existent password policies that allowed users to create insecure passwords. We observed password policies that:

- Allowed passwords to be as short as 3-characters
- Did not enforce password complexity
- Did not enforce maximum age or expiration of passwords
- Did not lock user accounts after numerous unsuccessful login attempts

What is the risk:

Weak password policies greatly increase the probability that brute-force or password-cracking attack will be successful, should they occur.

Specially designed password-cracking servers are capable of cracking the hashed value of any 9-character Windows password in under 30 seconds… Regardless of complexity.

Password Length	Average Time Required to Crack
≤ 9-characters	24 seconds
10-characters	10 minutes
11-characters	4.5 hours
12-characters	4.5 days
13-characters	120 days
14-characters	N/A - results in error

Over the course of this assessment, the use of weak passwords allowed our team to capture and successfully crack approximately 20,000+ user passwords. Additionally, the use of a weak password by a System Administrator not only allowed us to gain access to his account, but it also allowed us to completely disable two-factor authentication used at one of the universities.

How do we remediate:

The short answer is to enforce a strong password policy for all users.

However, we understand that password policies are not necessarily on-size-fits-all.

To be effective, password policies must be tailored to meet specific requirements of each department/division, while simultaneously providing adequate protection for the network as a whole.

When considering a password policy, it is critical that it is consistently applied to all users of the network. Think of the old analogy of “a chain is only as strong as its weakest link”. This means your network’s overall password strength will only be as strong as the strength of your weakest password policy.

A password’s entropy, or the measurement of its predictableness, is primarily measured by its length and complexity. Complexity is achieved by using a variety of upper and lower-case characters as well as numbers and symbols.

Other factors that increase entropy are:

- Password Age / Expiration
- Password Reuse
- Account Lockout
- Account Lockout Duration

While we cannot dictate a password policy, a suggested password policy is defined below:

Password Length:
Since the success-rate of password-cracking drastically decreases when passwords reach 13-characters in length, we suggest enforcing the following minimum password length for:

- Normal Users: 14-character minimum
- Privileged Users: 16-character minimum
- Service Accounts: 25-character minimum

Password Complexity:
Passwords should contain at least 3 of the 4 following character sets:

- Upper Case
- Lower Case
- Number
- Symbol

Password Expiration:
Since 13-character passwords can be cracked in 120 days, we suggest passwords used for both normal and privileged accounts expire after 90-days. Service accounts, due to their nature are not required to expire.

Password expiration is vital in protecting the network. Should a password become unknowingly compromised, the password expiration policy limits the amount of time a compromised password can be used.

Password Re-use:
Users should not be allowed to reuse a password previously used within the last 2-years.

Account Lockout:
Accounts should be locked and/or disabled after 3 to 5 consecutive unsuccessful authentication attempts.

Account Lockout Duration:
Accounts should remain locked and/or disabled for at least 30-minutes or until a System Administrator unlocks it after verifying a user's identity.

** NOTE: Third-party software can also be deployed in order to ensure that the user's desired password doesn't match commonly used or known phrases, and isn't included on popular breeched-password lists.

ES02: NDIT RESPONSE

NDIT Response:	
Item (1):	Enforce a strong password policy for all users
Response (1):	NDIT and Enterprise Architecture (EA) maintains federally compliant password policies for all agencies that must abide by EA policy. Agencies or governmental entities that do not fall under EA may have policies that vary including having passwords that do not expire. In these instances, NDIT does not have the authority to mandate non-EA Entities have passwords in accordance with the EA password policy. Requiring all entities to follow EA password requirements would require the Legislature to provide NDIT with the statutory authority to mandate EA password requirements for all nd.gov users. The updated EA Password Policy moves state users to be in line with the recommendation and will move the character minimum from 8 to 15. Privileged users will be moved to 20 characters to maintain compliance with CJIS requirements The EA password policy has been developed based on NIST guidance and requirements that the State needs to follow to protect critical information systems.

ES02: NDUS RESPONSE

NDUS Response:	
Item (1):	Enforce a strong password policy for all users
Response (1):	The password requirements currently in place for NDUS accounts meet or exceed the recommendations in NIST Special Publication 800-63B – Digital Identity Guidelines. Currently, NDUS accounts require a 12-character password, which exceeds the 800-63 recommendation of 8-character, however, based on the recommendation in this finding, a 14-character password will be considered. The recommendations in these findings are somewhat in conflict with 800-63, specifically as it relates to password complexity and expiration. Also, authentication to many of the systems and services NDUS provides require multifactor authentication which limits the risk of stolen or compromised credentials. Finally, many of the insecure password policies identified in the findings are local policies and accounts at NDUS member institutions, which will need to be addressed.

ES03: SEPARATE ACCOUNTS NOT USED FOR PRIVILEGED ACTIVITIES

What we observed:	Testing encountered users performing privileged and non-privileged activities using the same account.
What is the risk:	Privileged accounts (i.e. Admin Accounts) are capable of performing restricted tasks such as account creation, configuration changes, and password resets for others. Privileged accounts that become compromised by malware, or a malicious attack, give the attacker full access to the system. The more times a privileged account is used, the more likely it is to become compromised. We performed numerous Man-in-the-Middle attacks where credentials from network users were easily captured. On several occasions, the captured credentials had administrative access, which in turn gave us the ability to leverage the privileged access held by that account to further exploit network resources.
How do we remediate:	Users that require privileged access should be provided two separate accounts. One account will have the ability to perform privileged "administrative" operations, and the other should be a non-privileged or "standard" user account. • The privileged account should only be used when privileged actions such as hardware installation, configuration changes, or account maintenance are required. • Users should perform all other "non-privileged" daily activities using their non-privileged "standard-user" account.

ES03: NDUS RESPONSE

NDUS Response:	
Item (1):	Users that require privileged access should be provided two separate accounts
Response (1):	How NDUS and member institutions manage and monitor Privileged (Admin) accounts is a known gap that needs to be addressed by NDUS in coordination with member institutions. This may require process changes and/or implementation of specific Privileged Account Management technology solution(s).

ES04: INSECURE LEGACY PROTOCOLS

What we observed:	Testing observed the wide-spread use of insecure legacy protocols.
What is the risk:	Legacy protocols are susceptible to Man-in-the-Middle and/or Spoofing attacks where valid credentials are captured and/or stolen before being relayed to the original network destination, completely unbeknownst to the end-user. Testing efforts consistently exploited these protocols throughout the entire assessment. Three of the four individual networks that were completely compromised during testing, occurred as a direct result of exploiting these protocols. Additionally, 10 of the 13 networks tested during this assessment utilized these protocols and are 100% vulnerable to this attack.
How do we remediate:	Remediating this attack requires that legacy protocols be disabled. In order to disable these protocols, all computers on the network must be correctly configured and capable of using DNS to perform lookup and name resolution requests. ITD has attempted to disable these protocols in the past, but computer systems at a supported agency are still dependent of these legacy protocols to function properly. These legacy protocols cannot be disabled until the dependent systems are upgraded.

ES04: NDIT RESPONSE

NDIT Response:	
Item (1):	Legacy protocols in use
Response (1):	NDIT is aware of the insecure legacy protocols noted in the detailed report. Currently, there is at least one legacy agency system that will not allow for the upgrade of these protocols in the enterprise. As a result, NDIT is unable to upgrade the protocols for the enterprise without causing significant issues with the legacy system.

ES04: NDUS RESPONSE

NDUS Response:	
Item (1):	Legacy protocols in use
Response (1):	NDUS acknowledges these legacy protocols need to be disabled, where possible, and will require both network and computer configuration changes across the university system.

ES05: CRITICAL DATACENTER INFRASTRUCTURE NOT PROTECTED WITH PHYSICAL BARRIERS

What we observed:	Critical power and cooling infrastructure was located in close proximity to the roadway. These components did not have adequate physical barriers to protect them from an accidental or deliberate car strike.
What is the risk:	Backup generators, and HVAC equipment are critical to the datacenter's continuous operation. If this infrastructure were to be damaged by an accidental or deliberate car strike, the datacenter would not be able to provide adequate cooling or power. While the generators were part of a redundant backup system that is only used in the event of a power-outage, the HVAC equipment is responsible for maintaining safe temperature and humidity levels and is a vital component of the datacenter's normal daily operation. Should a failure of HVAC systems occur, computing systems would have to be taken offline to avoid heat-related damage until a temporary cooling or power solution could be deployed.
How do we remediate:	Install security bollards or decorative boulders in strategic locations around critical HVAC and generators in order to prevent damage from a vehicle.

PHOTO SHOWING BOTH BACKUP GENERATORS AND HVAC EQUIPMENT (BEHIND FENCE). WHILE THE FENCE IS OF SUFFICIENT STRENGTH TO DETER VANDALS OR THIEVES FROM TAMPERING WITH THE EQUIPMENT, IT IS NOT STRONG ENOUGH TO PREVENT A VEHICLE FROM CRASHING THROUGH AND DAMAGING THE COOLING EQUIPMENT.

ES05: NDUS RESPONSES

NDUS Response:	
Item (1):	Datacenter not fully protected
Response (1):	NDUS has implemented significant physical security controls to protect the Datacenter facility including access controls, security alarms, surveillance cameras, redundant and backup power, fire detection and suppression, and temperature and humidity controls. NDUS does acknowledge that additional physical security barriers for external power and cooling infrastructure would reduce risk to the datacenter facility.

ES06: MISCONFIGURED WIRELESS NETWORK (NDUS GUEST)

What we observed:	Wireless testing at NDUS/CTS discovered that internal NDUS network resources were visible / accessible to users connected to the guest wireless network. Users connecting to the guest network could potentially access areas only meant for NDUS employees.
What is the risk:	The pre-shared password required to access the guest network was posted on conference room walls and freely shared with visitors. The password was also visible through windows located on the exterior of the building. This gave virtually anyone, who wanted to connect, access to the guest network as well as internal NDUS resources. Additionally, visitors were able to connect wirelessly to the guest network from the hotel adjacent to the NDUS/CTS offices.
How do we remediate:	Deploy Access Control Lists (ACL) or firewall rules that prevent users on the guest network from accessing internal network resources. Users connecting to the guest network should only have access to the Internet. **NOTE: This issue was immediately addressed and remediated by NDUS/CTS staff.

ES06: NDUS RESPONSE

NDUS Response:	
Item (1):	Limit user access
Response (1):	NDUS acknowledges the guest wireless network did give access to internal network resources, but not sensitive datacenter systems or servers which are protected by additional layers of security. As noted in the findings, this guest wireless network has been decommissioned and therefore the issue remediated.

ES07: UNAUTHENTICATED SMTP RELAY + REMOTE SHELL = PHISHING

What we observed:	Vulnerability scanning revealed a handful of unauthenticated SMTP Relay (E-mail) servers located on various subnets of the ITD and CTS network. Additionally, scanning found a vulnerability within an externally accessible device that gave attackers a remote shell to the internal network.
What is the risk:	By first exploiting the flaw discovered on the externally accessible device to get a remote shell to the internal network, testers were then able to relay phishing emails through the unauthenticated SMTP Relay discovered during vulnerability scanning. By relaying phishing emails through internally trusted email relay servers, testers were able to impersonate and mimic actual user accounts in ways that were undetectable to end-users. Since the email servers being used were both internal and trusted, phishing emails sent through them were not tagged with the "External Message" warning banner that gets added to the top of all incoming emails. Fake emails were sent to a random selection of NDGOV and NDUS employee's. These emails claimed immediate action was needed, and directed recipients to fake websites setup at https://verify.ndgov.us and https://verify.ndus.us, respectively. The fake websites were designed to mimic actual websites used by ITD and NDUS, and trick recipients into entering their passwords. Phishing Stats (24-hour period):

	# of Phishing Emails Sent	User Clicks	Passwords Captured
ITD	698	76 (11%)	63 (9%)
NDUS	730	199 (27%)	153 (21%)

	**PLEASE NOTE: For statistical reference, NDUS allowed their phishing campaign to run an additional 24-hours. This resulting in the capture of 22 additional user clicks and 12 additional passwords. In total, the NDUS phishing campaign captured 221 (29%) user clicks and 165 (23%) user passwords.
How do we remediate:	Ensure all SMTP relay servers are configured to only accept emails from authenticated users or known/trusted IP addresses (i.e. – Printers & Web Servers). Continue to educate end-users on how to detect phishing emails.

ES07: NDIT RESPONSE

NDIT Response:	
Item (1):	Unauthenticated SMTP Relays
Response (1):	These relays are only used internally. Steps are currently being taken to further lock down their use to only systems that are approved.

ES07: NDUS RESPONSE

NDUS Response:	
Item (1):	Unauthenticated SMTP Relays
Response (1):	The SMTP (Email) server identified was only used internally, however, NDUS acknowledges that this server should be configured to only accept emails from authenticated users or known/trusted IP addresses, as do other NDUS SMTP (Email) servers in our environment.

ES08: EXTERNALLY EXPOSED NETWORK RESOURCES

What we observed:	Testing discovered a large number of network devices, management consoles, and services that were unnecessarily exposed and accessible to the public-facing internet. Examples of network devices that were accessible were: • Security Cameras • Printers • Audio Visual Equipment (Projectors, TV, Conference Gear) • Phones • Thermostats • Time Clocks Administrative and Remote Management Consoles: • Firewalls • Switches • Storage Arrays • Wireless (WiFi) Network Controllers • Backups • Remote Desktops Services • SSH • Power Distribution Units Several of these devices and consoles were still configured with a default username and password. Testing also discovered one rogue web proxy (SQUID), that allowed external users to access internal university resources in addition to other internally connected NDUS networks. Testing also observed constant stream of Chinese and Russian IP addresses probing and conducting brute-force password attacks on internal resources.
What is the risk:	All devices have weaknesses and vulnerabilities that could allow them to be exploited. When devices are exposed to the public internet, you allow hackers, bots, and script-kiddies from around the world an opportunity to attack and potentially compromise that device. Depending on the severity of the vulnerability, an exploited device could result in anything from a minor disruption in service, to a full compromise of the internal network. Hackers and automated bots are constantly scouring the internet in search of exposed devices and services. Once discovered, a brute-force attack will often be launched against the device in an attempt to guess the password. Devices with default or weak password can be quickly guessed. Complex passwords can be compromised when given enough time. Simply put, an increased number of publicly accessible devices/services directly equates to additional risk.
How do we remediate:	Conduct periodic scans of external networks to identify exposed resources, and ensure additional unknown devices haven't appeared. Secure all access to all administrative consoles requires a VPN connection, or ensure access is limited to a known set of whitelisted IP addresses.

ES08: NDIT RESPONSE

NDIT Response:	
Item (1):	External Facing devices
Response (1):	NDIT is actively taking steps to remediate

ES08: NDUS RESPONSE

NDUS Response:	
Item (1):	External Facing devices
Response (1):	NDUS and its member institutions have a large IP address space, and therefore a large public-facing Internet footprint to protect. This offers many challenges, especially since many of our systems need to be public facing to serve our constituents. NDUS has made progress on reducing this footprint, and NDUS does currently conducts scans of external networks to identify exposed resources. However, NDUS does acknowledge that coordination with Institutions is necessary to develop additional capabilities to identify resources unnecessarily exposed to the Internet in order to move them to private networks and/or further protect the resource.

ES09: PATCHING AND CONFIGURATION MANAGEMENT

What we observed:	While it was obvious that coordinated vulnerability scanning and patch management programs were in place, testing still uncovered a considerable number of Critical, High, and Medium vulnerabilities and security misconfigurations while scanning the network. While we were able to successfully exploit a handful of discovered vulnerabilities, a solid defense-in-depth strategy rendered many of our attacks unsuccessful. Even though several devices and services were confirmed to have known vulnerabilities, additional protection mechanisms such as firewalls, anti-virus, and endpoint protection software were responsible for halting the attack.
What is the risk:	Out-of-date and unpatched software/firmware contain known vulnerabilities that can be easily compromised. A compromised device could allow malicious insiders or hackers to gain unauthorized access to network resources.
How do we remediate:	Dedicate more resources to patching and flaw remediation. Isolate and restrict access to devices that are unable to be patched or updated. Decommission / Retire devices or software that are unable to be patched.

ES09: NDIT RESPONSE

NDIT Response:	
Item (1):	Dedicate more resources to patching and flaw remediation.
Response (1):	NDIT has recently created a formal Vulnerability Management Program for addressing risk. To date the following actions have been taken: • A Vulnerability Oversite Group has been created to oversee the program and address remediation of vulnerabilities. • A formalized program has been developed for VMP • Service Now tool implementation is on track for completion by mid-July

ES09: NDUS RESPONSE

NDUS Response:	
Item (1):	Dedicate more resources to patching and flaw remediation.
Response (1):	NDUS has been improving and expanding its vulnerability management program over the past several years, however NDUS acknowledges that more resources need to be dedicated to the patch and vulnerability management programs.

ES10: STAGENET DOESN'T REQUIRE ACKNOWLEDGEMENT OF A USE POLICY / LOGIN BANNER

What we observed:	Users connecting to the STAGEnet wireless network were not required to authenticate, or acknowledge an acceptable-use policy or login-banner.
What is the risk:	Login banners provide a definitive warning to any possible intruders who access your system that certain types of activities are illegal or not allowed. This warning also advises authorized and legitimate users of their obligations relating to the acceptable use of the wireless environment. Without being required to acknowledge a login banner / acceptable use policy, users could claim plausible deniability to avoid prosecution for illegal activities.
How do we remediate:	Deploy a captive portal that verifies a user's email address and requires them to acknowledge a login banner and/or acceptable use policy before being allowed to connect to the network.

ES10: NDIT RESPONSE

Item (1):	Deploy a captive portal for wireless network
Response (1):	NDIT is reviewing this finding to determine its viability. Before deploying a captive portal for the wireless network NDIT must review the legal constraints, technical requirements, feasibility and other potential issues. NDIT will work with both legal counsel and the technical experts to determine whether a captive portal for the wireless network can be implemented.

8.8. KUDOS & COMPLIMENTS

Kudos, or a congratulatory notation, presents an opportunity for our team to acknowledge a strength that we noticed during our assessment. This item can be a configuration setting that defeated an attack, a design approach that is above average, or a methodology that improves security across the board.

SECURITY TEAM'S KNOWLEDGE AND UNDERSTANDING OF THEIR ENVIRONMENT

The world of Information Security is ever-changing and unpredictable at best.

- Network environments change on a daily basis…
- New vulnerabilities are discovered on a daily basis…
- And who can forget our favorite user, who always manages to click, change, download, or delete something they shouldn't… (on a daily basis)

Contending with these factors while simultaneously keeping the network secure is no easy task.

Finding the balance between functionality and security is a virtual tight-rope, that security professionals must walk every day.

If you tighten the security screws down too tight, users can't do their jobs. If you don't tighten them enough, your network becomes vulnerable.

Sometimes the solution is clear, sometimes the solution is a work-around, and sometimes the risk simply outweighs the solution – but the one thing you can always count on, is that the solution will never be the same.

That is why it is vital to have a Security Team that not only knows the network inside and out, but is equally familiar with the needs and requirements of their user-base.

- We saw these traits in the NDIT and NDUS teams on a daily basis.
- We saw two core teams that not only had awareness of any significant issue we brought to them, but already had customized solutions or roadmaps in place.
- We saw two teams equipped with enough technical diversity to handle any situation presented to them.
- We saw two teams that were open and receptive to ideas on improvement.
- Most importantly, we saw two teams that embraced this exercise as a learning experience, and something that could make them stronger.

We would like to personally thank Uriah Burchinal, Brad Miller, Bryan Ford, and Michael Roue for their help in coordinating this assessment.

Their daily communications, positive attitudes, and constant involvement played a vital role in allowing us to stay on task.