

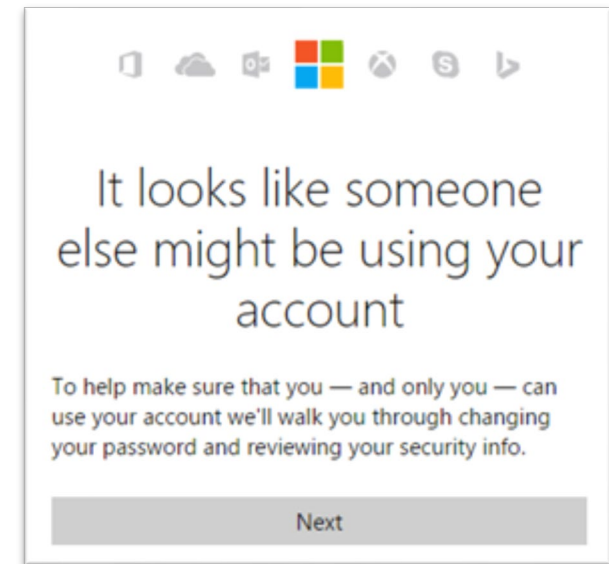
Study of Government Cybersecurity

CYBERSECURITY SERVICES - NETWORK

- Network Firewalls
 - Filtering,
 - Domain Name Service Security,
 - Virus Scanning, and
 - Traffic Inspection.
- Multi State Information Sharing and Analysis Center (MS-ISAC)
 - Domain Name Services,
 - National Collaboration.

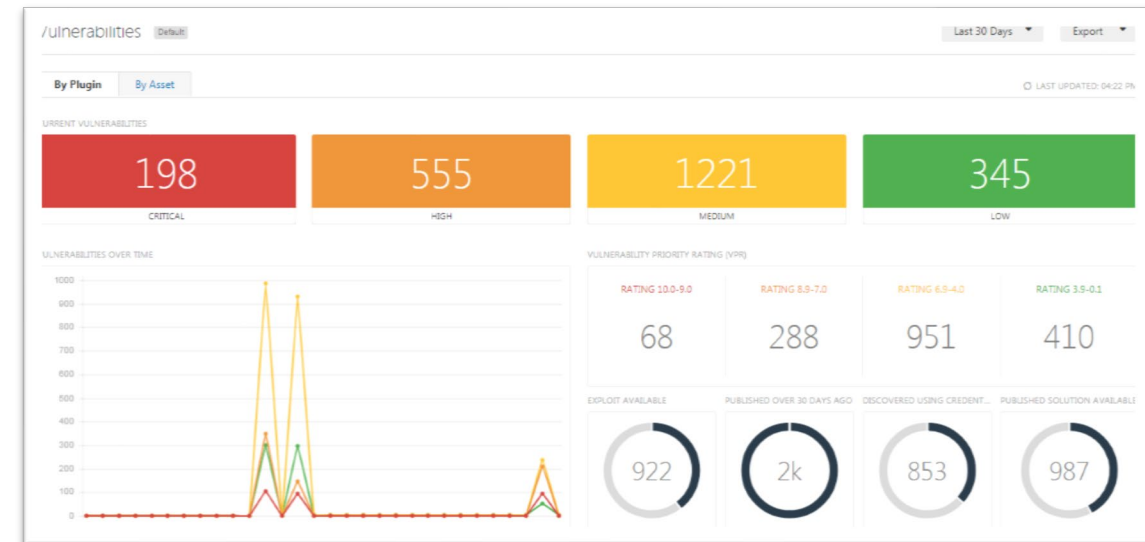
CYBERSECURITY SERVICES – DATA CENTER AND PLATFORM

- Zero Trust Network Deployment
- Defense in depth data center
- Office 365
 - Mail Protection
 - Data Loss Prevention
 - External File Sharing
 - Identity Protection (Impossible log-in, risky log-in)
- Multi Factor Authentication



CYBERSECURITY SERVICES – END POINT

- Endpoint Detection and Response (EDR)
 - Anti-Malware
 - Enables remote incident response
 - Shares to "State View" of cybersecurity
- Vulnerability Management
 - Detects vulnerabilities on systems
 - Detects vulnerabilities in applications



CYBERSECURITY SERVICES – ADMINISTRATIVE

- Cybersecurity Training
 - Phish Testing
 - Cybersecurity Training
- Threat Hunting
 - Detects active threats on network
 - Shared threat feeds from partners (state, local, tribal)
- Cyber Policy
 - Governance for secure implementation of systems
 - Governance for secure behaviors on network
- Risk Assessment
 - Assess security posture of systems
 - Assess security posture of third-party vendors



CYBERSECURITY SERVICES - INFORMATION

- Darkweb Monitoring
 - Scans for compromised North Dakota emails
 - Detects leaked credentials
 - Detects Leaked Personal Information
- Data Loss Prevention - Detects shared sensitive information

Search Results: 23857

Date	Leak Name	Values Emails (Redacted)	Passwords (Redacted)
Aug 04 2021	July 2021 Compilation Combo List	pj@nd.gov	il6
Aug 04 2021	July 2021 Compilation Combo List	dt@nd.gov	as
Aug 04 2021	July 2021 Compilation Combo List	gl@nd.gov	ma p
Aug 04 2021	July 2021 Compilation Combo List	tr@nd.gov	ni il
Aug 04 2021	July 2021 Compilation Combo List	gl@nd.gov	ko
Aug 04 2021	July 2021 Compilation Combo List	fo@nd.gov	y2

CYBERSECURITY SERVICES - ROLLUP

Type	Service	Unified Agencies	Non-Unified Agencies	K-12	Higher Ed	Counties	Cities	Comment
Network	Firewall	Yes	Yes	Yes	Yes	Yes	Yes	Inherited from STAGENet
	MSISAC	Yes	Yes	Yes	Yes	Yes	Yes	Inherited from STAGENet
Data Center	Zero Trust	Yes	Partial	No	No	No	No	Inherited from NDIT Data Center
	Office 365	Yes	Yes	No	No	No	No	Inherited from NDIT's O365
	Multi Factor Auth	Yes	Yes	No	No	No	No	Inherited from NDIT's O365
End Point	EDR	Yes	Partial (Slow Adoption)	Partial	Partial	Partial	Partial	Inherited from NDIT's EDR Product
	VulnManagement	Yes	Partial (Slow Adoption)	Partial	Partial	Partial	Partial	Inherited from NDIT's Vulnerability Management Product
Administrative	Cybersecurity Training	Yes	Yes	Partial	Partial	Partial	Partial	Inherited from NDIT's Training Product
	Threat Hunting	Yes	Yes	Yes	Yes	Yes	Yes	Inherited from STAGENet - Improves with more users
	Cyber Policy	Yes	Yes	No	No	No	No	Policy only for state agencies - Exploring SITAC Policy
	Risk Assessment	Yes	No	No	No	No	No	Risk Management Program for Unified Agencies
Information	Darkweb Monitoring	Yes	Yes	No	No	No	No	Requires use of A North Dakota Based Domain
	Data Loss Prevention	Yes	Yes	No	No	No	No	Need to use NDIT's O365

CYBERSECURITY SERVICES – DESIRED STATE

Type	Service	Unified Agencies	K-12	Higher Ed	Counties	Cities	Comment
Network	Firewall	Yes	Yes	Yes	Yes	Yes	Inherited from STAGENet
	MSISAC	Yes	Yes	Yes	Yes	Yes	Inherited from STAGENet
Data Center	Zero Trust	Yes	No	No	No	No	Need to reside in NDIT Data Center
	Office 365	Yes	No	No	No	No	Need to use NDIT's O365
	Multi Factor Auth	Yes	No	No	No	No	Need to use NDIT's O365
End Point	EDR	Yes	Yes	Yes	Yes	Yes	Need to use NDIT's EDR Product
	VulnManagement	Yes	Yes	Yes	Yes	Yes	Need to use NDIT's Vuln Product
Administrative	Cybersecurity Training	Yes	Yes	Yes	Yes	Yes	Need to use NDIT's Training Product
	Threat Hunting	Yes	Yes	Yes	Yes	Yes	Inherited from STAGENet - Improves with more users
	Cyber Policy	Yes	Yes	Yes	Yes	Yes	Policy only for state agencies - Exploring SITAC Policy
	Risk Assessment	Yes	No	No	No	No	Risk Management Program for Unified Agencies
Information	Darkweb Monitoring	Yes	Yes	Yes	Yes	Yes	Requires use of A North Dakota Based Domain
	Data Loss Prevention	Yes	No	No	No	No	Need to use NDIT's O365

CYBERSECURITY SERVICES – CURRENT PROJECTED EXPENSES

Tools	Network	Data Center	End Point	Administrative	Information	Sub Total
Endpoint Detection and Response	\$1,000,000.00	\$-	\$3,500,000.00	\$3,909,905.00	\$-	\$8,409,905.00
Vulnerability Management	\$-	\$39,000.00	\$798,000.00	\$3,235,040.00	\$-	\$4,072,040.00
Cybersecurity Awareness and Training	\$-	\$-	\$-	\$1,374,055.00	\$-	\$1,374,055.00
Monitoring	\$119,800.00	\$1,184,000.00	\$117,000.00	\$3,593,770.00	\$4,162,400.00	\$9,176,970.00
Cyber Risk Management	\$-	\$-	\$-	\$4,029,348.00	\$-	\$4,029,348.00
					Total	\$27,062,318.00

CYBERSECURITY SERVICES – CURRENT FUNDING

Type	Unified Agencies	K-12	Higher Ed	Counties	Cities
Network	Endpoint Fees	K-12 General Fund	Endpoint Fees	Endpoint Fees	Endpoint Fees
Data Center	Technology Fee	General Fund	General Fund	General Fund	General Fund
End Point	Technology Fee	General Fund	Endpoint Fees & General Fund	General Fund	General Fund
Administrative	Endpoint Fees Technology Fee	General Fund	Endpoint Fees	General Fund	General Fund
Information	General Fund	General Fund	General Fund	General Fund	General Fund

CYBERSECURITY SERVICES – DIVIDING COST

What metric should be used?

60 State Agencies

- 10,000 Endpoints
- Majority of Data Hosted
- Majority of Third-Party Risk

Risk Assessments?

178 K-12 Organizations

- 160,000 Endpoints
- PowerSchool Data Hosted

11 HE Institutions

- Endpoints managed by Higher Ed
- Network connections to campuses
- PeopleSoft Data Hosted

Training?

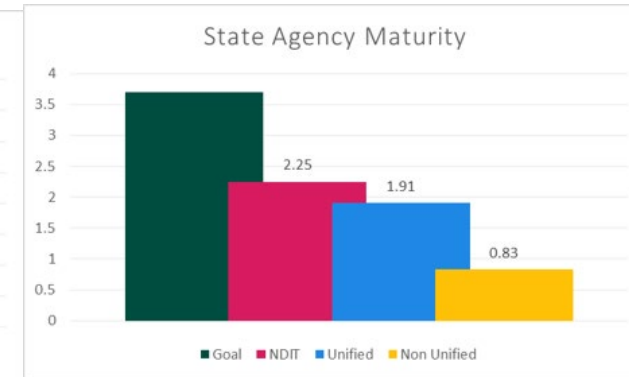
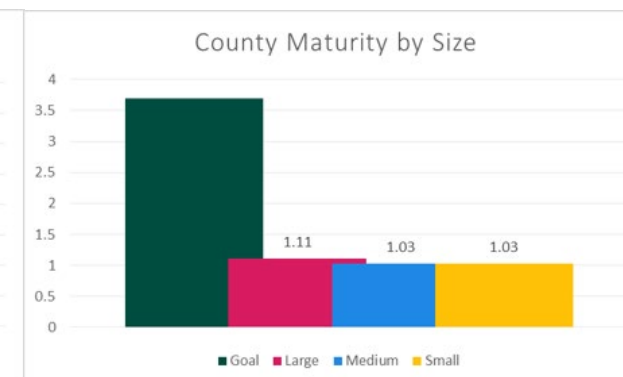
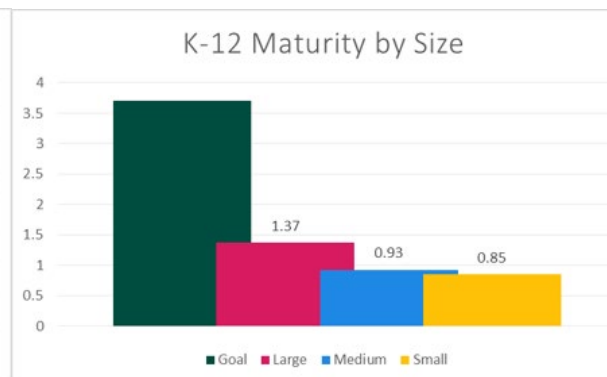
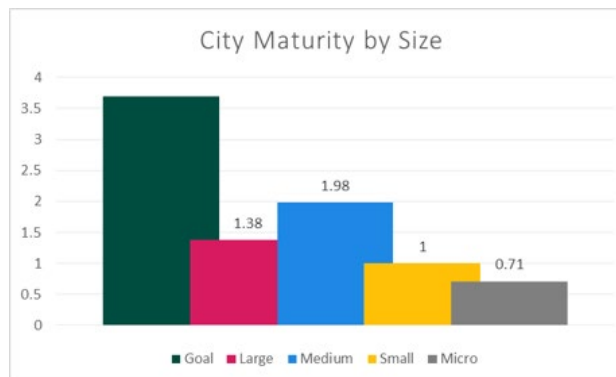
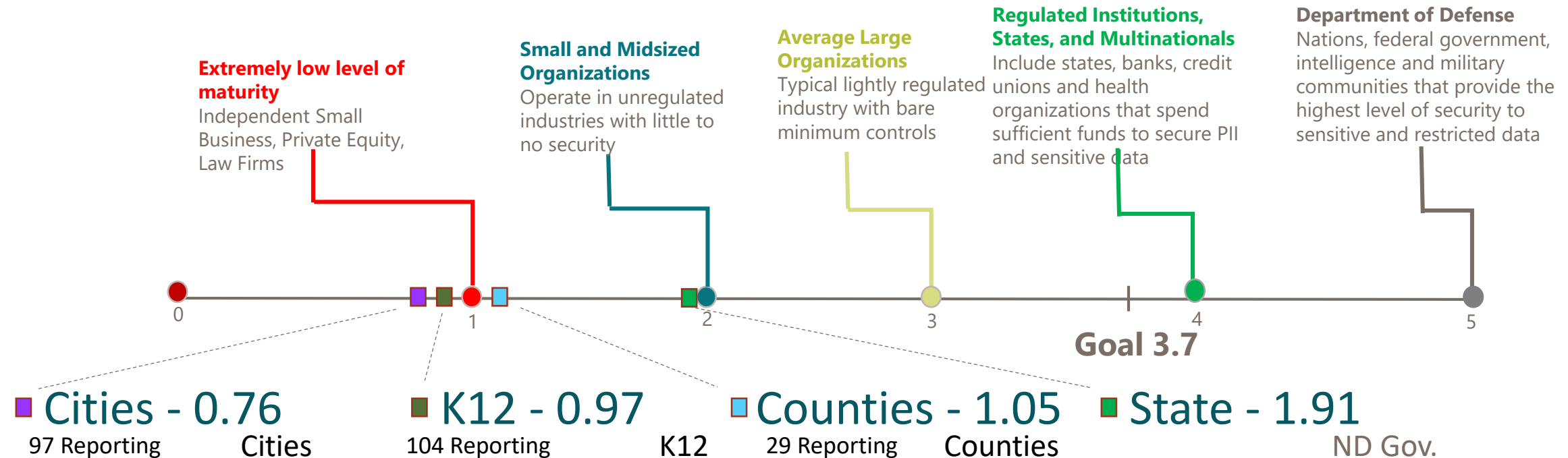
451 Municipalities

- 398 Cities
- 53 Counties
- 12,000 Endpoints
- Minimal Data Hosted

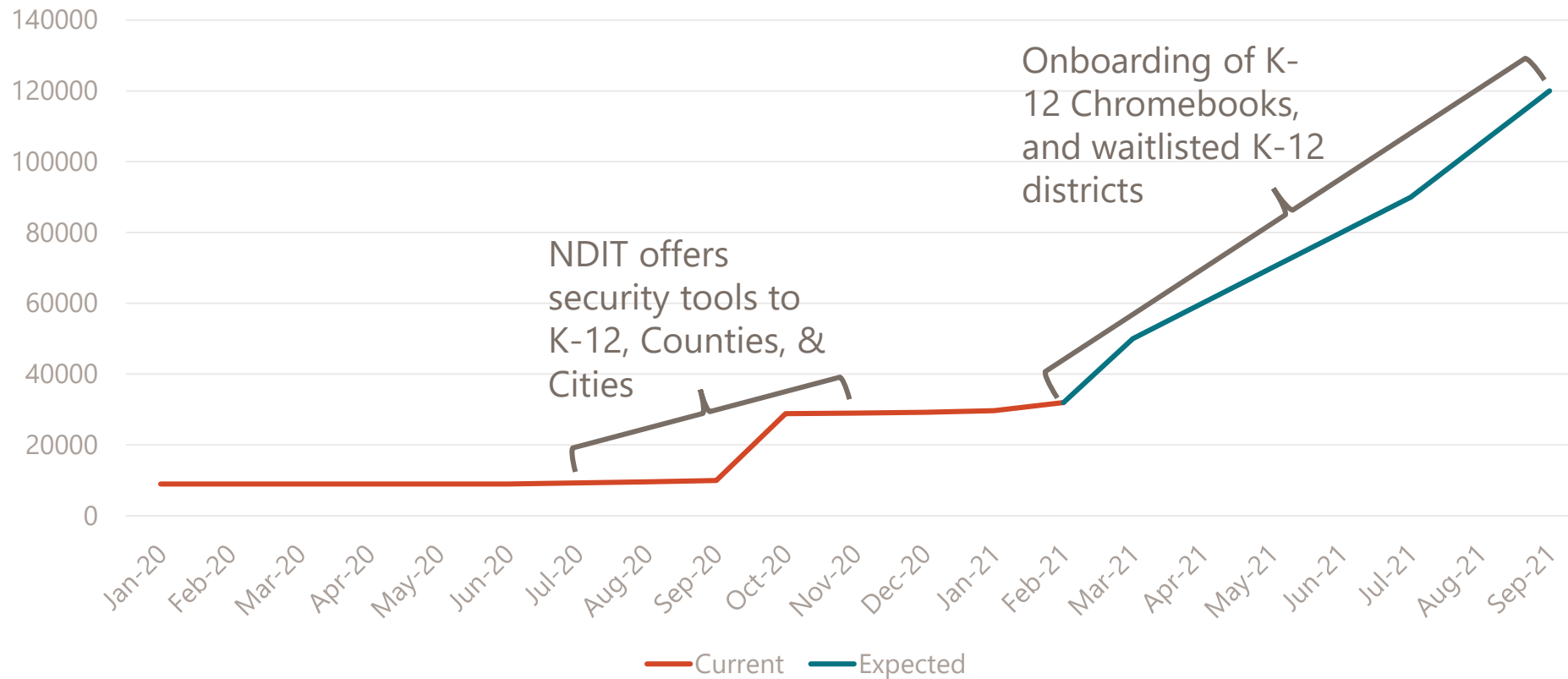
Cyber Policy?

CYBERSECURITY CAPABILITIES IN NORTH DAKOTA

42% overall participation rate (target 25%)



4X GROWTH OF SECURITY PRODUCT ADOPTION IN 2021



EXPENSE OF A NON-UNIFIED APPROACH

- The total cost in tools and services for every County, City, and School District in North Dakota to obtain basic security functionality would be **\$422,519,454.22¹** per Biennium.
- The total personnel required to fill the open positions is **6 times larger than the total yearly number of Computer Science Graduates in the State²** in a state that has more than 500 open computer science jobs.³

1. Based on Endpoint Detection and Response Toolset and Vulnerability Management Toolset quotes from 11/24/2020 for small government organizations (see Appendix) and industry average Security Analysts per endpoint from: Osterman Research - The Evolving State of Network Security, 2018, Cited by InfoSecurity group (September 2018). <https://www.infosecurity-magazine.com/news/security-staffing-low-in-midsized/>

2. Based on 152 bachelor's degrees in Computer Science per year from: Code.org North Dakota State Fact Sheet (2018). <https://code.org/advocacy/state-facts/ND>

3. Based on 506 open computing jobs (3.3 times the average demand rate in North Dakota) from: Code.org North Dakota State Fact Sheet (2018). <https://code.org/advocacy/state-facts/ND>

THREATS AND CONCERNS

- Information regarding cybersecurity targets, threats, concerns, and breaches in state agency and political subdivision systems
 - Ransomware
 - Phishing
 - Critical Infrastructure Cybersecurity
 - Third Party Risk
 - Auditors Findings

THREATS AND CONCERNS: RANSOMWARE

RANSOMWARE AFFECTED PHILADELPHIA
SEPTA TRANSPORT PAYROLL, TIME KEEPING &
REAL-TIME SCHEDULE SYSTEM

University of Utah hit by ransomware, pays \$457K ransom

Haywood County Schools closed after Ransomware attack

Gosnell schools hit with ransomware attack

Knoxville shuts down IT network following ransomware attack

Cyber-Attack Downs Alabama County's Network

Cooke County in Texas apparently hit by gang using REvil ransomware

Texas Takes Second Ransomware Hit

DoppelPaymer Ransomware hits Los Angeles County city, leaks files

City of Olean Computers Hit With Ransomware

Cyber Attack Reported In Bluffton, South Carolina, Authorities Confirm

Ransomware attack hits Champaign-Urbana Public Health District

Louisiana's governor declared a state of emergency after a cybersecurity attack on government servers

are Strikes Third US College in a Week

Gadsden school district hit by ransomware for the second time

North Miami Beach Police Department Hit With Ransomware Attack

Data breach follows ransomware attack

School's out as ransomware attack downs IT systems

Town of Colonie got hacked; looks to avoid paying ransomware demand about \$400,000

Racine Mayor Refuses to Pay Cyber-Ransom

County's Computers Still Down Nine Days After Ransomware Attack

PBVSD ransomware attack will delay report cards

22 Texas Towns Hit With Ransomware Attack

Attack In 'New Front' Of Cyberassault

City Agrees to Pay Hackers \$600,000

Redcar cyber-attack: Council using pen and paper

Ransomware Takes Out Durham, North Carolina

North Miami Beach Police Department Hit With Ransomware Attack

Ransomware attack responsible for La Salle County technology issues

Mississippi City Operations Disrupted by Ransomware Attack

Second Florida city pays giant ransom to ransomware gang in a week

Hackers Are Holding Baltimore Hostage: How They Struck and What's Next

600 Computers Taken Down After Florida Library Cyberattack

Fort Worth ISD Hacked, Joining Other Texas Schools, Towns Hit by Ransomware Attacks

Cyber-Attack Makes Pennsylvania Students Learn "Old School" Style

Hackers demand Michigan school district ransom

Emergency Following Cyber Attack

Ransomware attack cancels classes at Three College

IT Technical College latest victim of ransomware

Texas attack: Garrison, Nacogdoches schools hit with ransomware

South Adams Schools hit with ransomware cyber-attack

THREATS AND CONCERNS: RANSOMWARE IN SUPPLY CHAIN

Ransomware has been an ongoing threat in supply chain

- Energy
- Agriculture



JBS paid \$11 million ransom after cyberattack

BY NICOLE SGANGA

UPDATED ON: JUNE 10, 2021 / 7:06 PM / CBS NEWS



What's the latest fallout from the Colonial Pipeline hack?

Answer: Some employees' personal information may have been compromised.

August 17, 2021 • News Staff



Fuel holding tanks are seen at Colonial Pipeline's Linden Junction Tank Farm on May 10, 2021, in Woodbridge, New Jersey. (Michael M. Santiago/Getty Images/TNS)
Michael M. Santiago/TNS

THREATS AND CONCERNS: CRITICAL INFRASTRUCTURE

- Directed attacks against critical infrastructure
- Cyber-physical systems
 - Increased impacts from cybers attacks,
 - Generally older systems.



RISK MANAGEMENT

NDIT Risk Management

- Evaluated for Risk
- Vendors-TPRM
 - Systems-RMF
 - Exceptions/Waivers

Vendor Risk

Tier or Residual Risk Rating	Reassessment Frequency	Documents to be Updated
Tier 0	Annually	<ul style="list-style-type: none">▪ Agency Head Verification of Services▪ New applicable <i>Security Survey(s)</i> Required▪ Data Security Certification Attestations
Tier 1 or Critical	Annually	<ul style="list-style-type: none">▪ Agency Head Verification of Services▪ New applicable <i>Security Survey(s)</i> Required▪ Data Security Certification Attestations
Tier 2 or High	Annually	<ul style="list-style-type: none">▪ Agency Head Verification of Services▪ New applicable <i>Security Survey(s)</i> if the surveys are significantly altered or change of services.▪ Data Security Certification Attestations
Tier 3 or Moderate	Biennially (every two years)	<ul style="list-style-type: none">▪ Agency Head Verification of Services▪ New applicable <i>Security Survey(s)</i> if the surveys are significantly altered or change of services.▪ Data Security Certification Attestations*
Tier 4 or Low	Triennially (every three years)	<ul style="list-style-type: none">▪ Agency Head Verification of Services▪ Data Security Certification Attestations*

System Risk (RMF)



THIRD PARTY RISK MANAGEMENT (TPRM)

- Process Workshops (OMB)
- Beta Testing-September 2021
- Evaluation of Current Vendors
 - ~1200
- Full Integration Into Procurement Anticipated July 2022

The Role of the China Chopper Webshell

```
1 rule webshell_chinachopper_nab
2 {
3   meta:
4     author = "Jeff White (Palo Alto Networks) @nootrak"
5     date = "20MAR2021"
6   strings:
7     $hash01 = "e8a017cd1d6d3389c792cce8c8ff1927a6386f9ef32ab0b97763de1f86ffc8"
8     $hash02 = "34f9944a85fba58f3f0b0c5dc32da1ce6743da26e1e1820ef6c419808757112"
9     $hash03 = "55fbfab29f9d2c26f81f1f901af8381807f76cc81f140791a8983a08b8425"
10    $hash04 = "6e79b0cd22ecbdf1c7796e381a3f88e30e82f5698c6b31b64d8f1e9cfdb67"
11  }
12  strings:
13    // Detect OAB file
14    $OAB01 = "ExternalUrl" ascii // Contains webshell
15    $OAB02 = "InternalUrl" ascii
16    $OAB03 = "ExchangeVersion" ascii
17    $OAB04 = "WhenChangedUTC" ascii
18  }
19  // Detect injected url variables
20  $SH1P01 = "http://f/" ascii nocase
21  $SH1P02 = "http://g/" ascii nocase
22  $SH1P03 = "http://p/" ascii nocase
23  // Detect ChinaChopper variables
24  $websh01 = "script language=JScript" ascii nocase
25  $websh02 = "script language=VBScript" ascii nocase
26  $websh03 = "script runtime=server" ascii nocase
27  // Detect webshell anchors
28  $cc01 = "Request" ascii nocase
29  $cc02 = "Page_Load" ascii nocase
30  // Detect injected pattern, no webshell
31  $ion = /http:\/\/[a-z]\.[a-z-0-9]*/
32  condition:
33    (all of ($OAB*) and 1 of ($SH1P*) and 1 of ($websh*) and all of ($cc*))
34  or
35  $ion =~ $ion
```

The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal

Isabella Jbilan and Katie Canales Apr 15, 2021, 12:25 PM



SolarWinds Corp. banner hangs at the New York Stock Exchange (NYSE) on the IPO day of the company in New York. Reuters/Brendan McDermid



The majority of data breaches and cyberattacks exploit third-party cyber gaps. The report found that in 2019, **44%** of companies experienced a **significant data breach** through a **third-party vendor**.

AUDITOR'S FINDINGS-PEN TEST

ES01-Critical	Full adoption and implementation of a formal Risk Management Framework	In progress: Awaiting personnel to implement (FTE)
	NDIT has to wait on the authority or approval to act upon a detected incident	Partially Resolved: Resolved for Unified Agencies
ES02-High	Enforce a strong password policy for all users	Partially Resolved: Resolved for Executive Branch Only
ES04-High	Legacy protocols in use	On Hold: Active Directory Upgrade Required (MMIS)
ES07-High	Unauthenticated SMTP Relays	Resolved
ES08-High	External Facing devices	Resolved
ES09-Medium	Dedicate more resources to patching and flaw remediation.	In Progress: Tools have been put in place and ARPA request for vulnerability remediation resources
ES09-Medium	Deploy a captive portal for wireless network	In Progress: Solutions are being considered

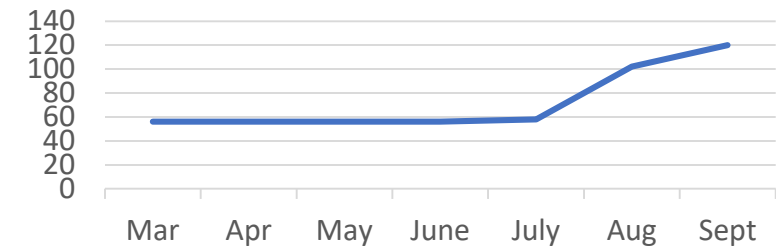
APPENDIX

Security

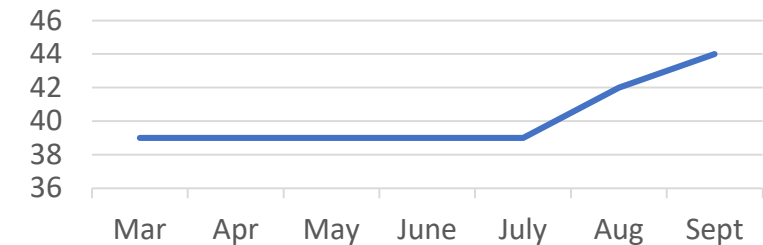
Whole of State Approach

- The number of K-12 Districts, Cities, and Counties supported by NDIT has **Doubled** since the COVID-19 outbreak;
 - 120 Districts total with more implementing,
 - Expect 75% of all K-12 districts using NDIT resources by mid-October,
- Similar increase in County and City Governments using NDIT resources;
- Deliver about **\$400 Million** in people, processes, and technology.

K12 Districts



Counties



North Dakota's Political Subdivisions

629 Total Political Subdivisions

- 178 K-12 Organizations
 - 160,000 Endpoints
- 451 Municipalities
 - 398 Cities
 - 53 Counties
 - 12,000 Endpoints
- 172,000 Endpoints Total
- 273 Mean Endpoints per PSD

Risk Calculations

Risk Formula:

*1 Year Risk = [(629 PSDs * **Exposure Factor**) * Average **Cost of Ransomware Response**] + Average **Cost of State Damages**

*Risk per biennium = Yearly Risk * 2

Where...

- **Exposure Factor**: 46% for US Public Sector Ransomware Exposure¹
- **Average Response Cost**: \$1,090,489 Average (50/50 payed & unpaid)²
 - Ransom not payed \$732,520
 - Ransom payed \$1,448,458
- **Average Cost of State Damages**: \$8,000,000 damages to government per ~160,000 Assets³

So...

$[(629 * 46\%) * (\$1,090,489)] + \$8,000,000 = \text{Yearly Risk: } \$323,522,087.26$

And...

Risk per biennium = $\$647,044,174.52$

1. Based on 46% exposure reported for Government Entities From: THE STATE OF RANSOMWARE 2020 Results of an independent study of 5,000 IT managers across 26 countries; Sophos Security (May 2020). <https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf>
2. Based on average cost to mitigate attack for both payed and unpaid ransoms from: THE STATE OF RANSOMWARE 2020 Results of an independent study of 5,000 IT managers across 26 countries; Sophos Security (May 2020). <https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf>
3. Baltimore estimates cost of ransomware attack at \$18.2 million as government begins to restore email accounts; Baltimore Sun (May 2019). <https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-ransomware-email-20190529-story.html>

Tool Cost Calculations Per PSD

\$149,000 Per Organization Per Year

- \$ 118,000.00 for Endpoint Detection and Response (Per Organization Per Year)
 - Quoted Palo Alto Networks 11/24/2020
- \$31,000 for Asset Vulnerability Management (Per Organization Per Year)
 - Quoted Highpoint Networks 11/25/2020

250 Endpoints				
SKU	Product	List Price for 12 Month Term	Quantity	Extended List Price
PAN-XDR-ADV-EP	Cortex XDR Pro for 1 endpoint, includes 30 days of data retention	\$70.00	250	\$17,500.00
PA N-LGS-1TB-1Y R	Cortex Data Lake with 1TB of storage, increases retention to 120 days (Assume 10TB per 250 devices)	\$2,000.00	10	\$20,000.00
PAN-XDR-MTH	Managed Threat Hunting Service for 250 endpoints	\$9,800.00	0.25	\$2,450.00
PAN-CORTEXXSOAR-ENTERPRISE	Cortex XSOAR is full product that includes automation, orchestration, and threat intelligence management for Enterprise (includes 4 user XSOAR licenses) Therefore assume .25 unit for 1 licenses	\$250,000.00	0.25	\$62,500.00
PAN-AF-1YR	AutoFocus Intelligence Service Standard subscription - one user	\$35,000.00	0.25	\$8,750.00
PAN-DEMISTO-PREMIUM-SUCCESS	Cortex XSOAR Premium Success - sold with Cortex XSOAR, XSOAR-TIM and XSOAR-Starter Therefore assume .25 unit for 1 licenses	\$50,000.00	0.25	\$12,500.00
PAN-CONSULT-RE-12MO	Resident Engineer Per Day (Assume 10 days per year) RE can serve as SOC analyst or implementation engineer or both	\$1,540.00	10	\$15,400.00
			One year	\$139,100.00

HIGH POINT NETWORKS™

Tenable IO Estimate 1000 Endpoints

Prepared for:
State of North Dakota
Attn: Kevin Ford
4201 Normandy St
Bismarck, ND 58501

Prepared by:
High Point Networks, LLC

Quote #: 102591
Version: 1
Delivery Date: 11/24/2020
Expiration Date: 12/24/2020

Tenable IO (1000 Assets)

Qty	Item	Description	Price	Ext. Price
1	6QG294	TENABLE.IO VULNERABILITY MGMT SVCS LICs PER ASSET (1000 Assets)	\$38,000.00	\$38,000.00
1	6QG296	TENABLE.IO VM CONTAINER STD SVCS TENABLE.IO VM CONTAINER	\$0.00	\$0.00
Subtotal:				\$38,000.00

Nessus

Qty	Item	Description	Price	Ext. Price
5	SERV-NES	NESSUS PROFESSIONAL ONPREM-ANNUAL SUB	\$2,511.00	\$12,555.00
Subtotal:				\$12,555.00

Quote Summary

Description	Amount
Tenable IO (1000 Assets)	\$38,000.00
Nessus	\$12,555.00
Total:	\$50,555.00

1. Methodology: Price is lowest quote from quotes provided directly by the vendor and 2 retailers for the same products provided by NDIT security. Does not include the cost of integration or support. Assumes average 270 endpoints per municipal organization.

Cyber Proposal

Serving ~250K North Dakotans

Funded Individually

Cost to State in tools and services for all government entities across North Dakota to obtain basic security functionality per Biennium

\$413,882,000.22¹

The Cyber staff required would be

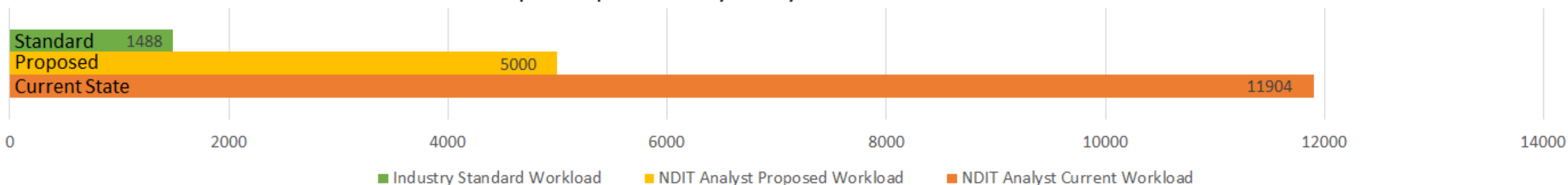
6 times the total yearly number of Computer Science Graduates in the State²

Through the Shared Service

Allows the state's shared service to support whole of government cyber in technology and people

- Special fund \$25.8m in recurring technology costs
- Add 29 FTE to the North Dakota IT Cybersecurity Team bringing the total analysts to **50**
 - **More than 3x the Operational Efficiency of the Average Fortune 500 Company³**

Workload – Computers per Security Analyst



1. Based on Endpoint Detection and Response Toolset and Vulnerability Management Toolset quotes from 11/24/2020 for small government organizations (see Appendix) and industry average Security Analysts per endpoint from: Osterman Research - The Evolving State of Network Security, 2018, Cited by InfoSecurity group (September 2018). <https://www.infosecurity-magazine.com/news/security-staffing-low-in-mid-sized/>

2. Based on 152 bachelor's degrees in Computer Science per year from: Code.org North Dakota State Fact Sheet (2018). <https://code.org/advocacy/state-facts/ND>

3. Based on industry average of 1 analyst per 1,488 endpoints for large organizations documented in Osterman Research - The Evolving State of Network Security, 2018, Cited by InfoSecurity group (September 2018). <https://www.infosecurity-magazine.com/news/security-staffing-low-in-mid-sized/>

Labor Cost Assumptions Per PSD

- At least \$180,000 per County/City/K-12 District
 - 1.44 FTE per organization to use the tools and respond to findings¹
 - Assumed IT FTE Cost of \$125,000 Per Year

1. Based on industry average of 1 analyst per 189 devices average for small organizations from: Osterman Research - Osterman Research - The Evolving State of Network Security, 2018, Cited by InfoSecurity group (September 2018). <https://www.infosecurity-magazine.com/news/security-staffing-low-in-midsized/>

Citations

- THE STATE OF RANSOMWARE 2020 Results of an independent study of 5,000 IT managers across 26 countries; Sophos Security (May 2020). <https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf>
- Baltimore estimates cost of ransomware attack at \$18.2 million as government begins to restore email accounts; Baltimore Sun (May 2019). <https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-ransomware-email-20190529-story.html>
- Osterman Research - The Evolving State of Network Security, 2018, Cited by InfoSecurity group (September 2018). <https://www.infosecurity-magazine.com/news/security-staffing-low-in-midsized/>
- Code.org North Dakota State Fact Sheet (2018). <https://code.org/advocacy/state-facts/ND>