



# Higher Education Committee

Darin King

NDUS Deputy CIO

Brad Miller

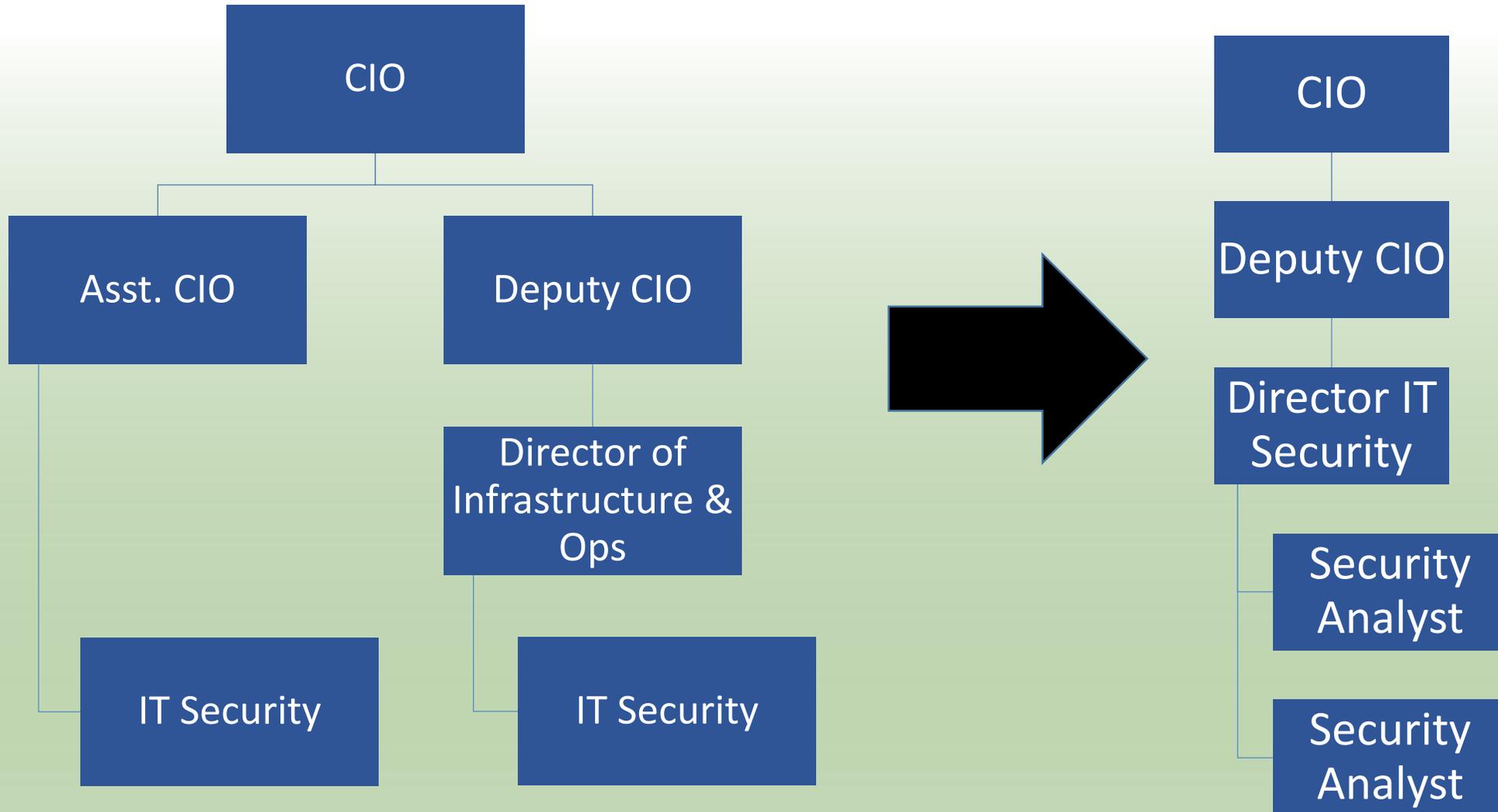
NDUS Director of Information Security



# NDUS Core Technology Services Agenda

- Security Status Update
- Strategic Security Plan
- Security Project Updates
- System Project Updates

# IT Security Organizational Restructure



# Intrusion Detection/Prevention

## Intrusion Detection/Prevention Systems Stats

September 2015 - March 2016

<i>Threat</i>	<i>9/30/15</i>	<i>10/31/15</i>	<i>11/30/15</i>	<i>12/31/15</i>	<i>1/31/16</i>	<i>2/29/16</i>	<i>3/31/16</i>	<i>Totals</i>	<i>Avg/Month</i>
<b>Vulnerability</b>	8,300,000	6,500,000	37,000,000	4,290,000	31,230,000	6,181,885	7,100,000	100,601,885	14,371,698
<b>Spyware</b>	3,800,000	70,200,000	5,300,000	4,430,000	7,940,000	914,937	1,840,000	94,424,937	13,489,277
<b>Virus</b>	16,400,000	19,000	556,000	16,540	10,700	14,631	32,700	17,049,571	2,435,653
<b>Wildfire</b>	31,500	34,900	67,000	154,240	15,570	56,037	43,000	402,247	57,464
<b>Scan</b>	687,700	64,500	556,000	503,650	62,660	320,952	24,300	2,219,762	317,109
<b>Flood</b>	1,800	281,600	1,200	736	1,010	1,410	240	287,996	41,142
<b>Totals</b>	<b>29,221,000</b>	<b>77,100,000</b>	<b>43,480,200</b>	<b>9,395,166</b>	<b>39,259,940</b>	<b>7,489,852</b>	<b>9,040,240</b>	<b>214,986,398</b>	<b>30,712,343</b>

# Intrusion Detection/Prevention

- StageNet Quads
  - Fargo, Grand Forks, Minot, Bismarck
  - Future state is an IPS/IDS device in front of each NDUS institution

# NDUS Information Security Strategic Plan



## Governance

### Program Charter

Mult-Factor  
Authentication

Endpoint  
Protection

Training  
and  
Awareness

Sensitive  
Information  
Discovery

Vulnerability  
Management

Centralized  
Logging

Policy

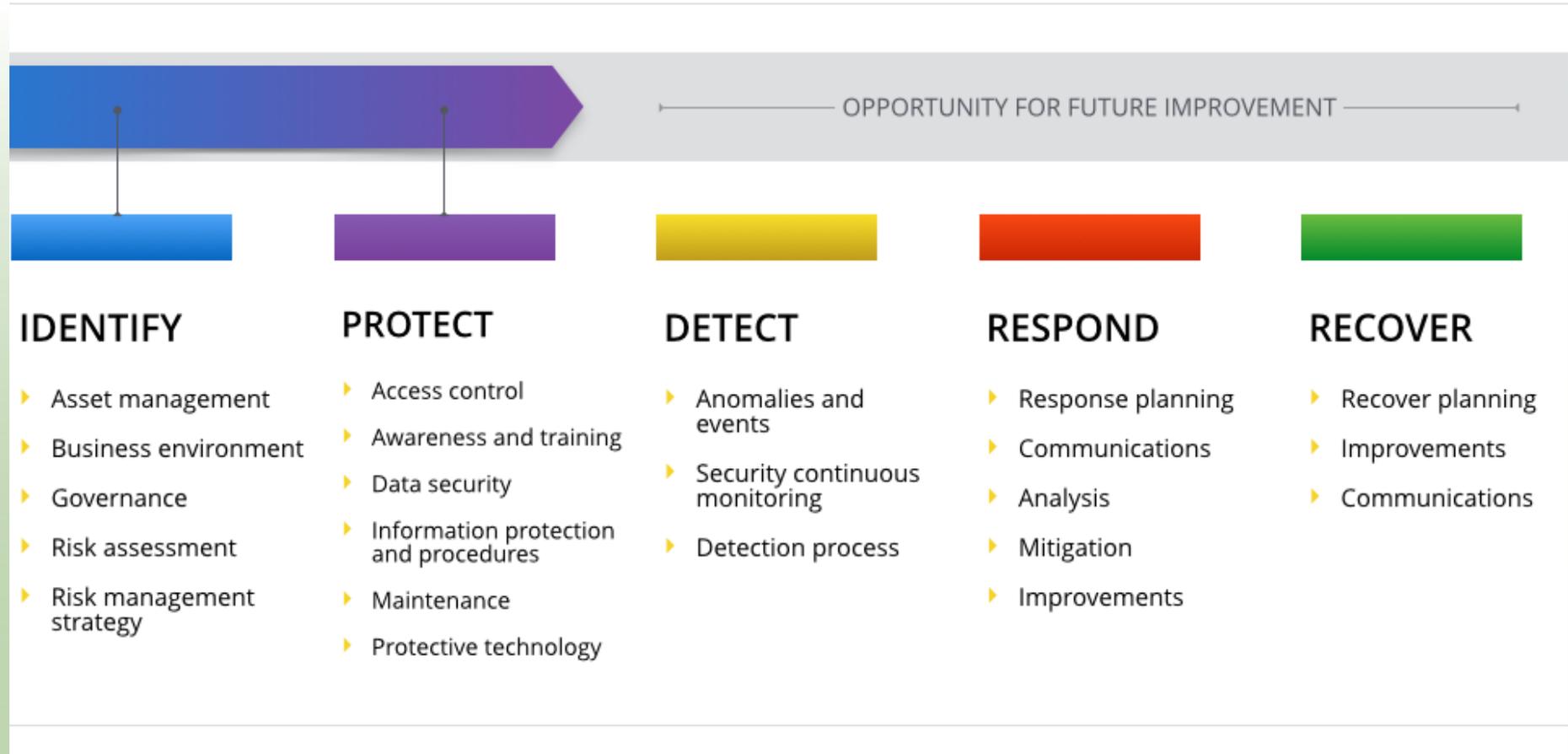
Standards

Procedures

Cybersecurity Frameworks and Standards

Data Classification

# Information Security



NIST Cybersecurity Framework Core

# Information Security

## Governance

- NDUS Information Security Council (ISC)
- CTS Information Security Group (ISG)

# Information Security



- Problems/Risks
  - Old outdated policy and standards
  - Need a data classification standard as a foundation for protection
  - No consistent understanding, implementation, and enforcement of policies and standards
- Benefits
  - Clear security baselines for all member institutions
  - Standards-based foundation to measure compliance and results
  - Consistent application of security controls based on data classification and system criticality



# Information Security



Information Security Policy Framework

# Information Security

## 1202 - Information Security Policy

1202.1  
Acceptable  
Use Policy

March 2016

1202.2  
Data  
Classification  
and IT  
Security  
Policy

June 2015

1202.3  
Data  
Privacy  
Policy

June 2016



# Information Security

## 1203 - Information Security Standards

1203.1  
Network  
Security  
Standard

Apr 2016

1203.2  
Server  
Security  
Standard

Aug 2016

1203.3  
Physical  
Security  
Standard

Oct 2016

1203.4  
Desktop  
Security  
Standard

Nov 2016

1203.5  
Incident  
Response  
Standard

Jan 2017

1203.6  
Disaster  
Recovery  
Standard

Mar 2017



# Information Security

## Multi-Factor Authentication

- Problems/Risks
  - 95% of breaches involve the exploitation of stolen credentials (2015 Verizon DBIR)
- Solution
  - NDUS is implementing a system-wide Multi-factor authentication solution
  - Already protecting over 10 services and expanding to campuses and Campus Solutions (Peoplesoft)
- Benefits
  - Reduces the risk of compromised NDUS credentials being used to gain unauthorized access to critical systems and data
  - Provides a notification mechanism for compromised credentials

# Information Security



## Endpoint Protection

- **Problems/Risks**
  - Many of the threats we face involve our endpoints (computers, laptops, servers) – phishing, malware, web browsing attacks, malicious email
- **Solution**
  - Need to implement advanced endpoint protection capabilities
  - An Endpoint Protection RFP and Procurement process is underway
- **Benefits**
  - Protect systems and data from known, advanced, and targeted malware and attacks
  - Identify attacks and malware infecting our endpoints in order to speed the remediation response once detected

# Information Security



Training  
and  
Awareness

- Problems/Risks
  - Protection of systems is not just a technical challenge – it relies on knowledge and action of the people within our organization.
  - Without proper training and awareness, faculty and staff become targets and not part of the solution.
- Solution
  - Create a security training and awareness program
  - A security awareness training program was procured and is currently being used in CTS and three campuses
- Benefits
  - Make individuals aware that the data on their computers is valuable and vulnerable
  - Empower individuals with the knowledge to be the first, and last, line of defense against security threats for protecting their systems and data

# Information Security



## Vulnerability Management

- Problems/Risks
  - All systems and applications are affected by vulnerabilities that are used by attackers to breach our environment
- Solution
  - Currently have deployed a system-wide vulnerability management system
- Benefits
  - Allows for the quick remediation of vulnerabilities on critical systems, network devices, and applications

# Information Security



## Centralized Logging

- Problems/Risks
  - Systems generate a large amount of log data that can be collected and analyzed to help identify, prevent, detect and recover from an attack.
- Solution
  - Currently deploying a log management system to centrally collect logs within the NDUS data center
- Benefits
  - Protects critical system logs from unauthorized access and modification
  - Provides a mechanism for log and event correlation to prevent, detect, and respond to a security incident

# Technology Project Updates

- Identity and Access Management
- Document Imaging
- Email Consolidation
- Functional Consolidation
- Data Inconsistencies

# Identity and Access Management

**Identity and access management (IAM)** is the security discipline that enables the right individuals to access the right resources at the right times for the right reasons.

*Gartner, retrieved April 13, 2016 from <http://blogs.gartner.com/it-glossary/identity-and-access-management-iam/>*

- Current/Future State Study
- Request for Proposal Created, Issued and Awarded
- Project Kickoff
- Ahead of schedule and under budget
- On target for a late October or early November production implementation



# Document Imaging Efficiency Update

- Two years into implementation – March 2014
- New infrastructure with dev, test, and production environments
- Completed
  - Migrated – UND, BSC, NDSCS, WSC (FA), MiSU, CTS Legacy,
  - On boarded – MaSU, LRSC, VCSU, DSU
- Work In Progress
  - Migrate – NDSU
  - On board –DCB, WSC (Records and Admissions)
- Project expected to be completed by June 2016
- Document Imaging Steering Committee established (2015)



# Document Imaging Efficiency Update

- Progress in Numbers
  - Active users (staff + some faculty) – 1380 (excluding NDSU, DCB, and WSC)
  - Storage and workflow applications – 124
- Key Applications
  - Admissions, Records, and Financial Aid in all 11 institutions
  - Accounts Payable and Purchasing at UND
  - Integration with PowerSchool (ITD) to feed high school transcripts
- Institutional Contracts Discontinued - \$165,898 (7 contracts)
- Next Steps (pending approval of steering committee and funding)
  - Onboard business offices including HR, Student Finance, Accounts Payable
  - Streamline transcripts processing by integrating with Campus Solutions

# Email Consolidation/Archiving

- Consolidation into single NDUS tenant underway for past year
- Rule based Archiving solution in NDUS tenant
  - 2 years per N.D.C.C.
- 7 of 11 campuses completed
  - UND, NDSCS, LRSC, DCB, WSC, BSC, DSU
- 2 campuses in progress
  - MaSU, MiSU
- 2 campuses in preliminary planning
  - NDSU, VCSU



# Functional Consolidation

## N.D.C.C. 15-10-44.1

- Document Campus IT Systems and Services
  - Campus Visits with Institutional Presidents and IT Staff
  - Multiple technical team discovery sessions with NDUS and institutional IT staff
- Develop NDUS Policy and Procedure
  - Currently being drafted simultaneously
  - Review and approval by SBHE
- Select and Prioritize Services to be Consolidated
  - Develop Business Cases
  - Develop Service Catalog
- Final Report December 2016

# Data Center

- Physical Space
  - Using 35% of raised floor
  - Using 50% of electrical capacity (includes cooling)
- Technical Architecture
  - 48 hosts and 508 virtual servers (80% capacity)
  - 350Tb storage (72% capacity)



# Data Inconsistencies

## HB 1003 Section 42

- HB 1003 identified 25 data inconsistencies among NDUS campuses
- Project management outsourced
- Project spread over four phases
  - Phase I – complete with two objectives carried into Phase II
  - Phase II – in progress
- Project Status – Red
  - Re-plan in process
  - New steering committee formed, chaired by NDUS Compliance Officer



# Thank You!

Questions?