



Walleyes, Whales & Cybersecurity

October 2, 2018

Speaker



Jim Edman

Deputy Commissioner and CISO
State of South Dakota

WALLEYES WHALES & CYBER SECURITY



South Dakota



Jim Edman
CISO
South Dakota

SD State Government

Statistics

Budget: \$4.7B

- General: \$1.6B
- Federal: \$1.7B
- Other: \$1.4B

FTE: 13,862

- 8,708 State Government
- 5,154 Higher Education

Miscellaneous

- 870,000 (#47)
- 77,184 sq miles (#17)
- State vs. Wayfair



SD State Government

What your tax dollar pays for



49¢

Education

- K-12
- Higher Ed.
- Tech Schools
- Dept of Ed.

36¢

Taking Care of People

- Medicaid
- DSS/DHS/DOH
- State Institutions

10¢

Protecting the Public

- Corrections
- Courts
- Public Safety
- Attorney General

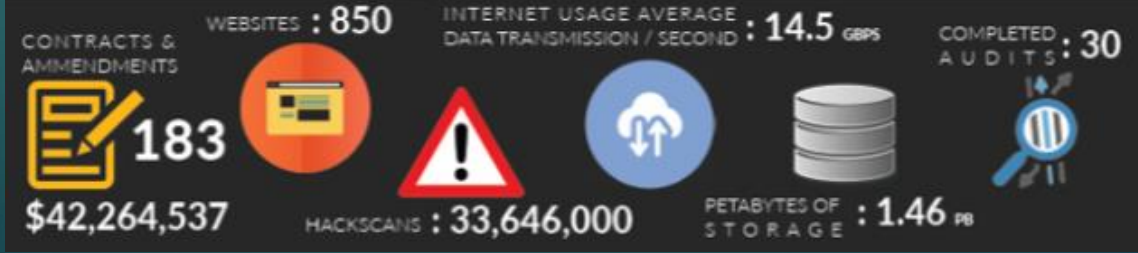
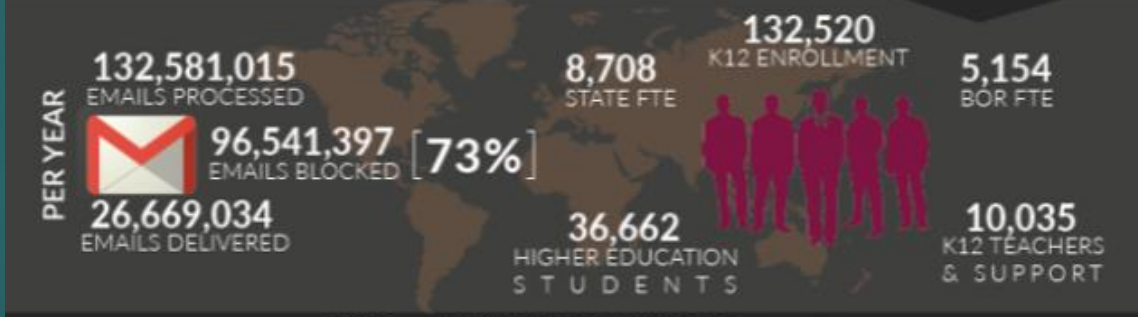
5¢

Rest of State Govt

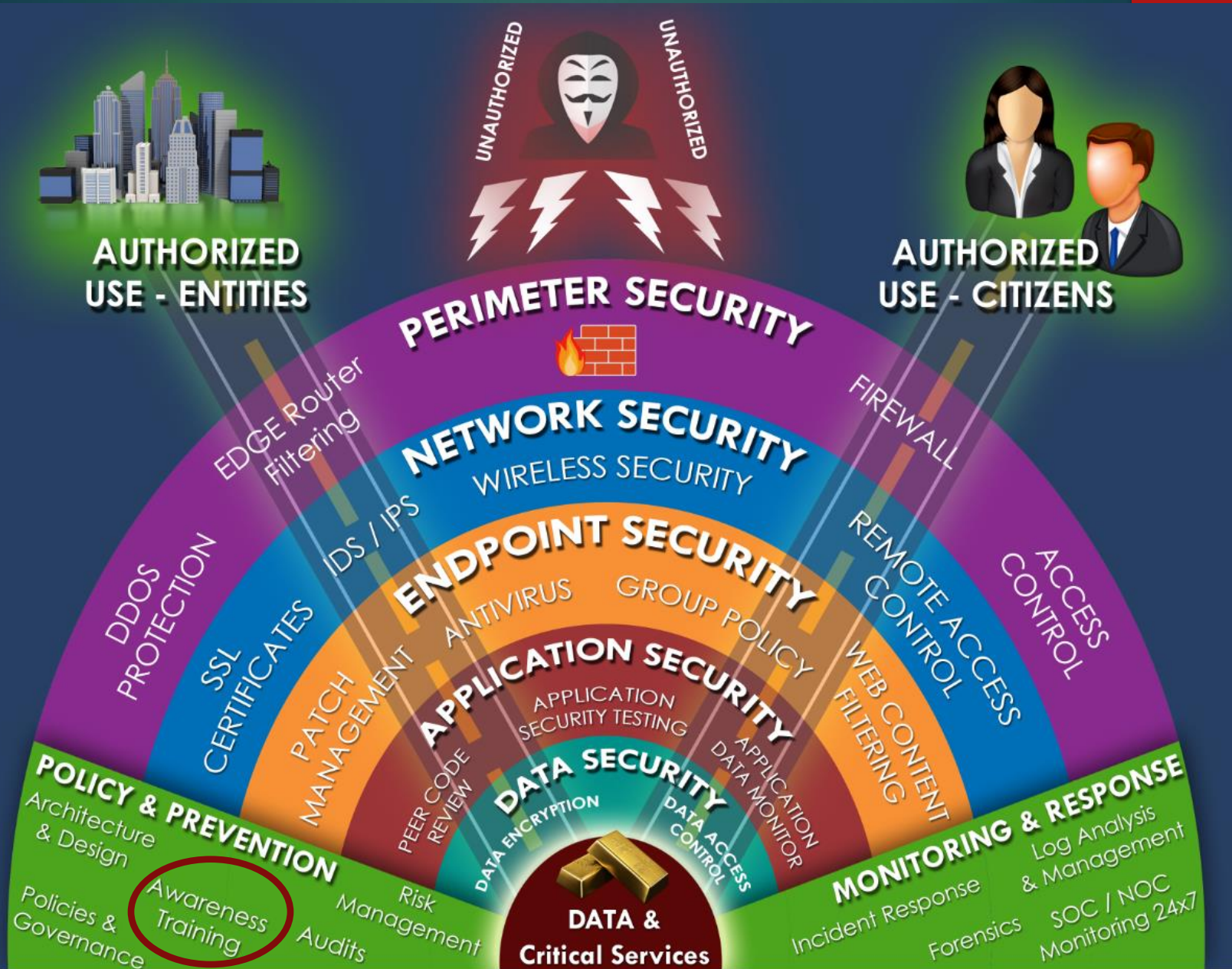
- 11 Dept's
- 4 Bureaus
- Legislature
- Governor
- 5 Const. Offices

Excludes Bond Payments

CYBER SECURITY SCOPE

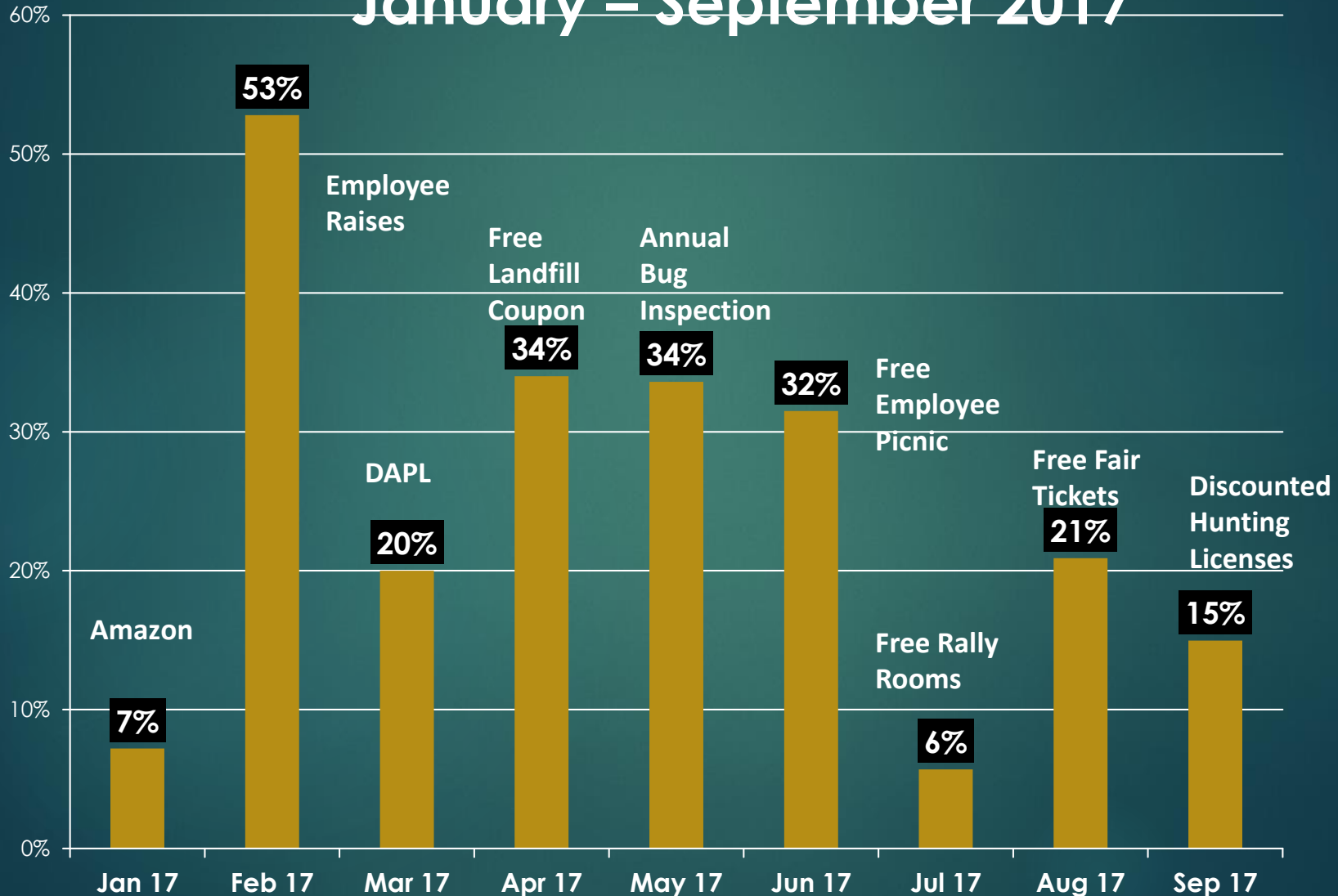


Cyber Infrastructure

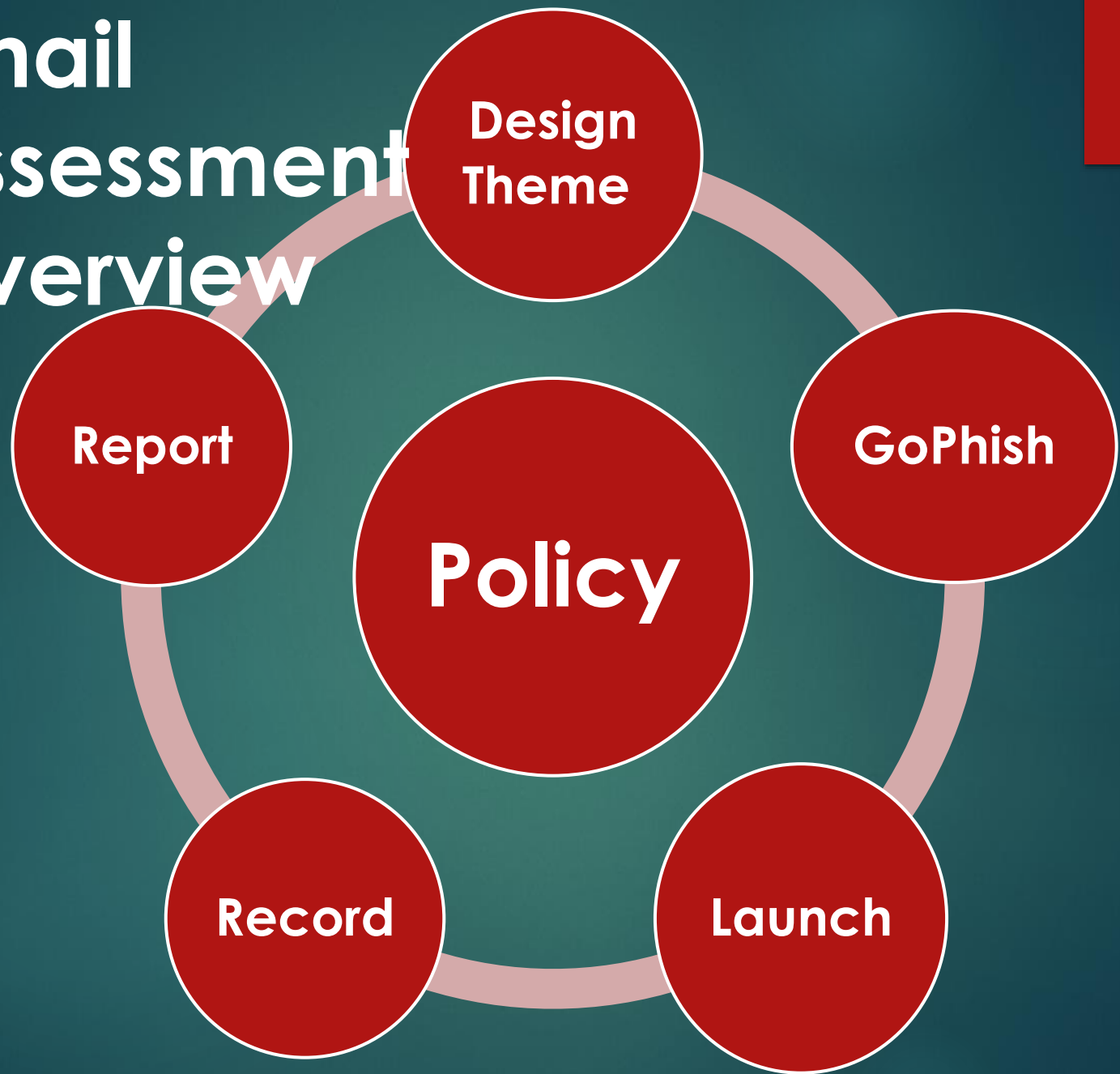


Problem:

Email Threat Assessment January – September 2017



Assessment Overview



Email Assessment Goals

1. Educate

- [EXT] in Subject:
- Do not hurry
- Be skeptical
- Review Sender
- Read Content
- Hover over links
- Question attachments
- Submit for sandbox detonation



2. Safeguard State Resources



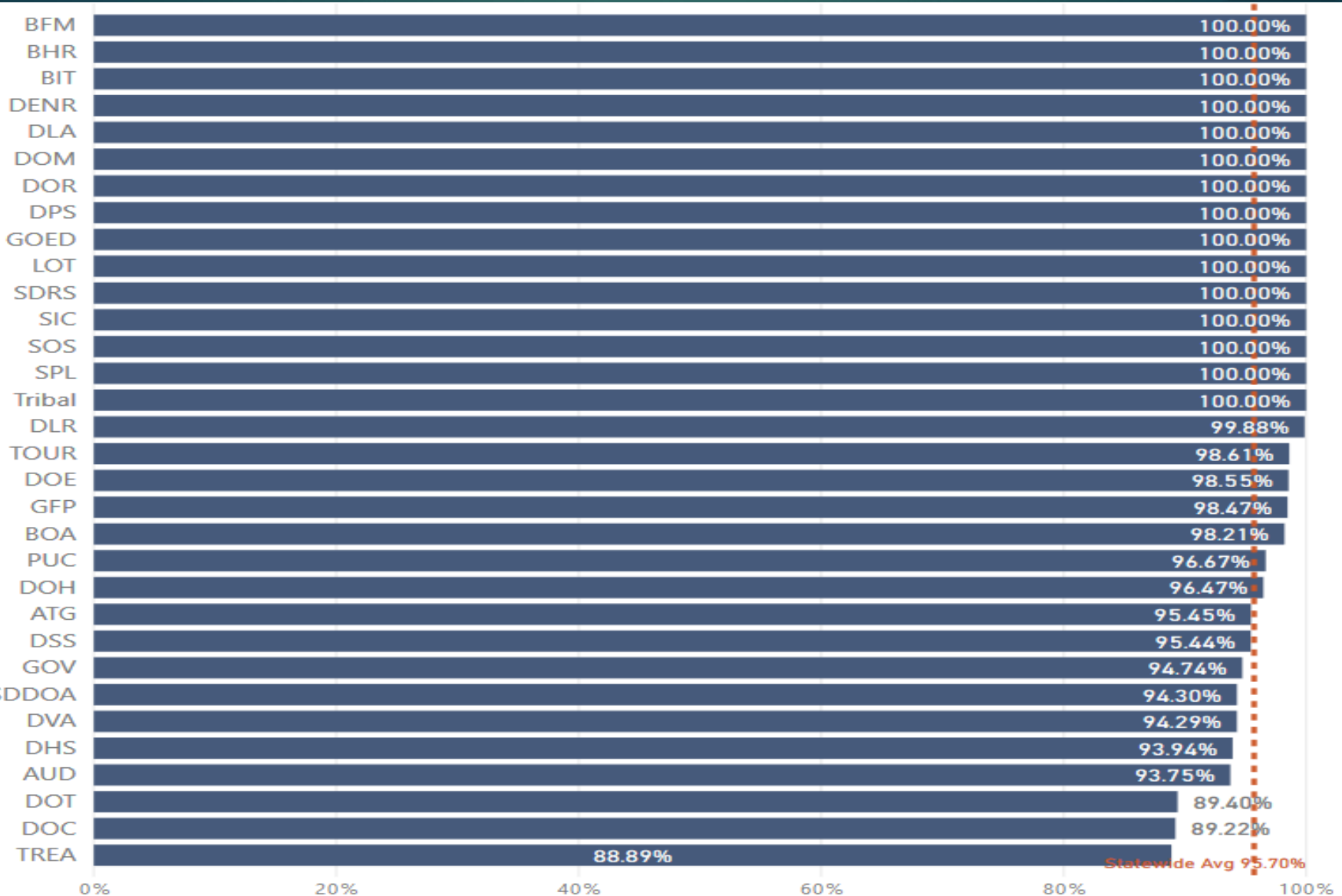
Cyber Security Policy

- Requires Employee Training
- Authorizes Assessments
- Consequences of offense(s):
 - 1st Nothing
 - 2nd Notification:
 - Individual
 - Department Head
 - 3rd Attend In Person training
 - 4th Account access review



Cyber Security Training

Statewide Completion: 96%



Design Theme

- **Ingest the Global Address List**
- **Design the message**
 - **Actual phishing messages received**
 - **Current – Emotional – Personal – Individual - Free**
 - **Pre-Approval ?**



Sample Message: Individual


Mon 01/08/2018 8:10 AM

GI Government Information <GovInfoSystem@state.sd.us>
[EXT] All State Employees REQUIRED to verify Info

To Edman, Jim (BIT)

Retention Policy Never Delete (Never) Expires Never

i You forwarded this message on 08/07/2018 9:02 AM.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.



Please verify your State Employee information

Beginning in 2018, it is necessary to verify your State computer account information. This is done to verify that your computer is adequately protected against computer malware. Please click on the link below. Your system will be automatically scanned using the latest desktop protection software. It will only take a few minutes and will not harm any of your files.

Email:	jim.edman@state.sd.us
First Name:	Jim
Last Name:	Edman

Please note that failing to complete this process will result in your account being locked.

By clicking on the button below you certify that the information you provide is correct and agree to the [Terms and Conditions](#).

Sample Message: Emotional



From: "KSFY News" donotreply@ksfy.com <"KSFY News" donotreply@ksfy.com>
Sent: Tuesday, March 8, 2016 11:00 AM
Subject: Breaking News



Legislators refuse State Employee Raise



In a stunning new development the Legislators have voted down a proposed raise to State employees that would increase employee wages by 5%.

For more on the story : <http://www.ksfy.com/home/headlines/>

Sample Message: Personal



Tue 08/14/2018 8:13 AM


UPS View <info404@ups.com>

[EXT] UPS Ship Notification

To ✓ Edman, Jim (BIT)

Retention Policy Never Delete (Never)

Expires Never

 You forwarded this message on 08/20/2018 11:05 AM.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

The physical parcel may or may not have actually been tendered to UPS for shipment.

The status of your package has changed. [View Status](#)

Shipment Details

From: South Dakota Government

Ship To: [\(Please Update\)](#)

Tracking Number: [1E53845416980121](#)

Number of packages: 3

Sample Message: Free

Reply Reply All Forward IM

Mon 08/14/2017 2:11 PM

State Fair <FreeTickets@state.sd.us>

[EXT] Free State Fair Tickets for State Employees

FREE SD State Fair Tickets







Looking for a day of fun? Love fair food, carnival rides, and music? Take a short trip over to the South Dakota State Fair in Huron, SD, and experience it all for free!

Enter your State ID at the link below for a FREE 4-Pack of Tickets to the <http://alert.sdgov-it.org?rid=nyoyxbs> e Fair!
Click to follow link

[Enter State ID Here](#)

Sample Message: Whale



Fri 09/14/2018 2:53 PM
 **Michels, Matt (Lt. Governor)**
Fwd: [EXT] Aaron Rodgers Out for Season
To:  Edman, Jim (BIT);  Venhuizen, Tony
Retention Policy 2 Year Delete (Default) (2 years) Expires 09/13/2020
 If there are problems with how this message is displayed, click here to view it in a web browser.

From: Green Bay Packers <news@gbpackers.com>
Date: September 14, 2018 at 2:53:31 PM CDT
To: Matt Michels <matt.michels@state.sd.us>
Subject: [EXT] Aaron Rodgers Out for Season

September 14, 2018



Aaron Rodgers Out for Season

Green Bay, WI

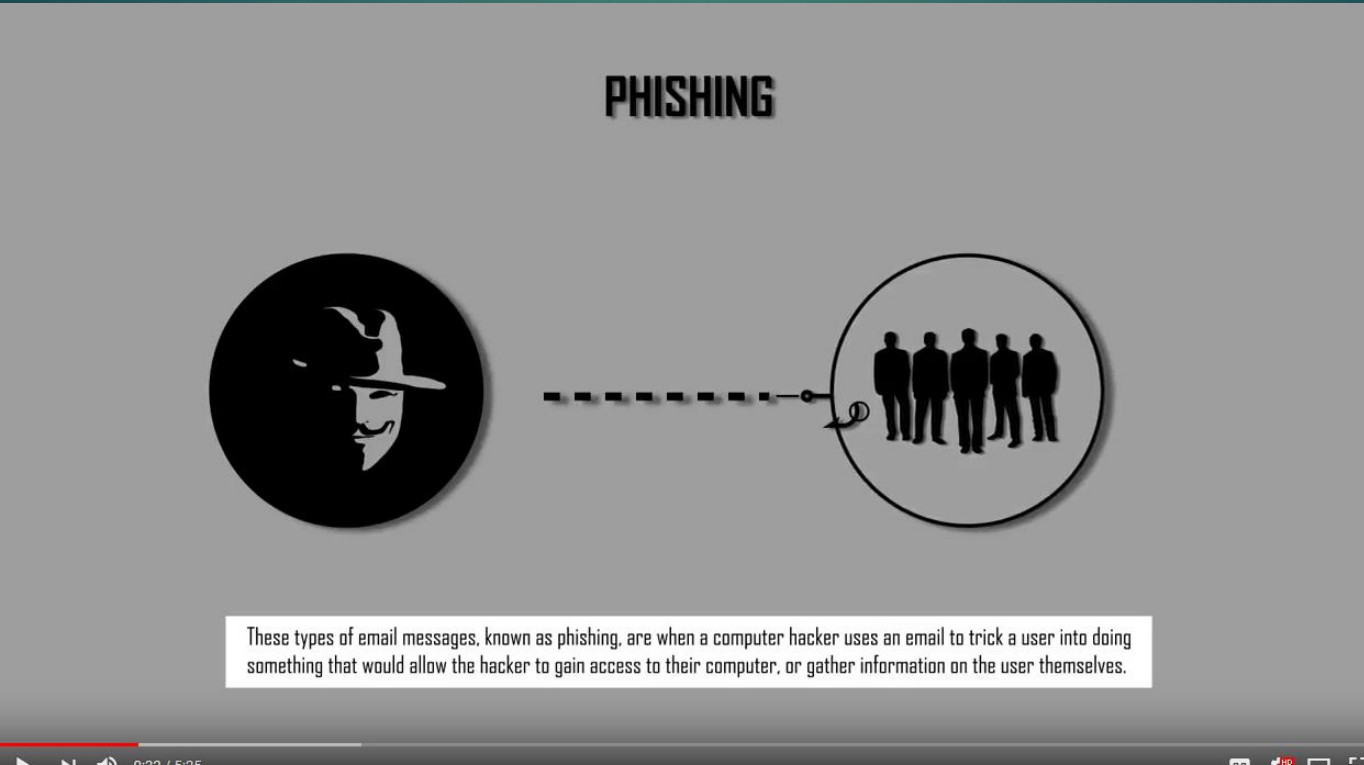
It was just announced by Green Bay Packers' coach Mike McCarthy that star quarterback Aaron Rodgers has a torn ACL and will miss the remainder of the NFL season.

The injury was suffered in Sunday night's win over the Chicago Bears. The entire press conference including x-rays of the injury can be found [here](#).

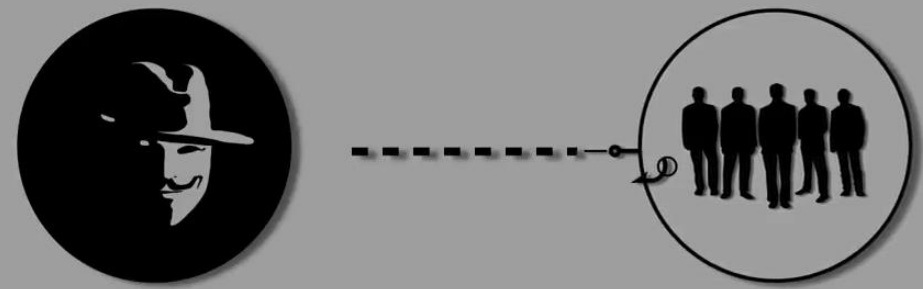


Configure GoPhish

- Build the Landing Page
- Update the video or web site
- Log recording



PHISHING



These types of email messages, known as phishing, are when a computer hacker uses an email to trick a user into doing something that would allow the hacker to gain access to their computer, or gather information on the user themselves.

0:32 / 5:25

CC HD

Launch the Campaign

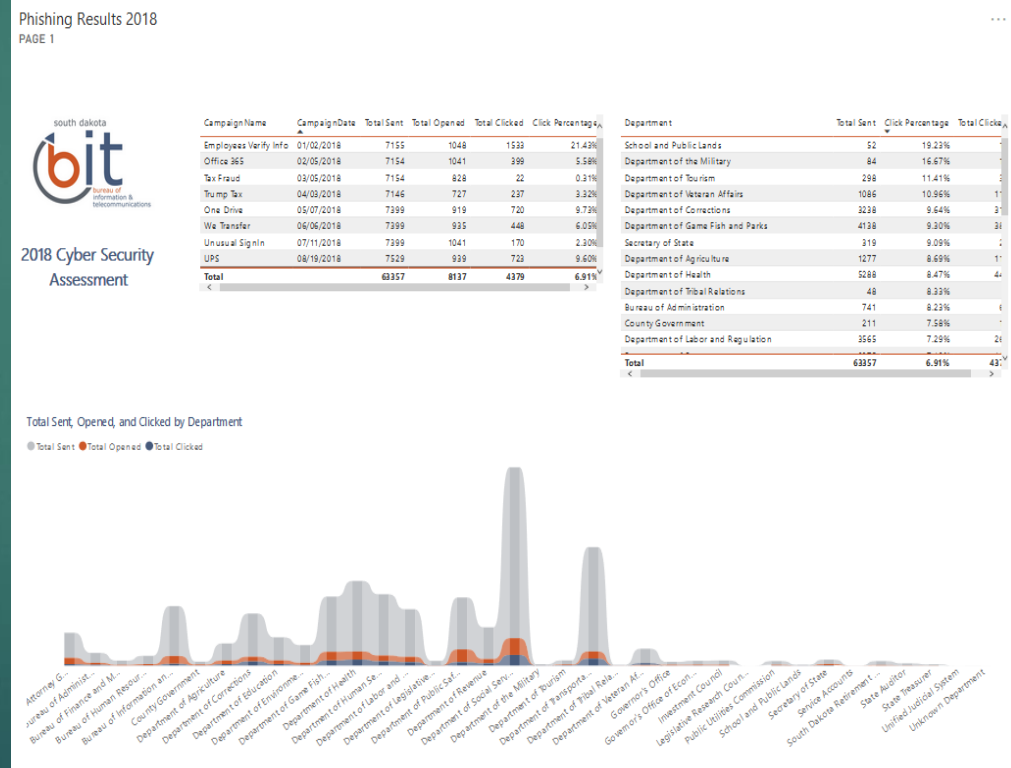
- **Monthly**
- **Executive Branch & Constitutional Offices**
- **Unified Judicial System?**
- **No Legislative Branch**
- **7,200 – 7,600 messages**
- **Delivered over 3 weeks**
- **Vary days of week messages delivered**

Record

- **Web server logs**
- **Ingested into Access**

❖ Statistical Gathering

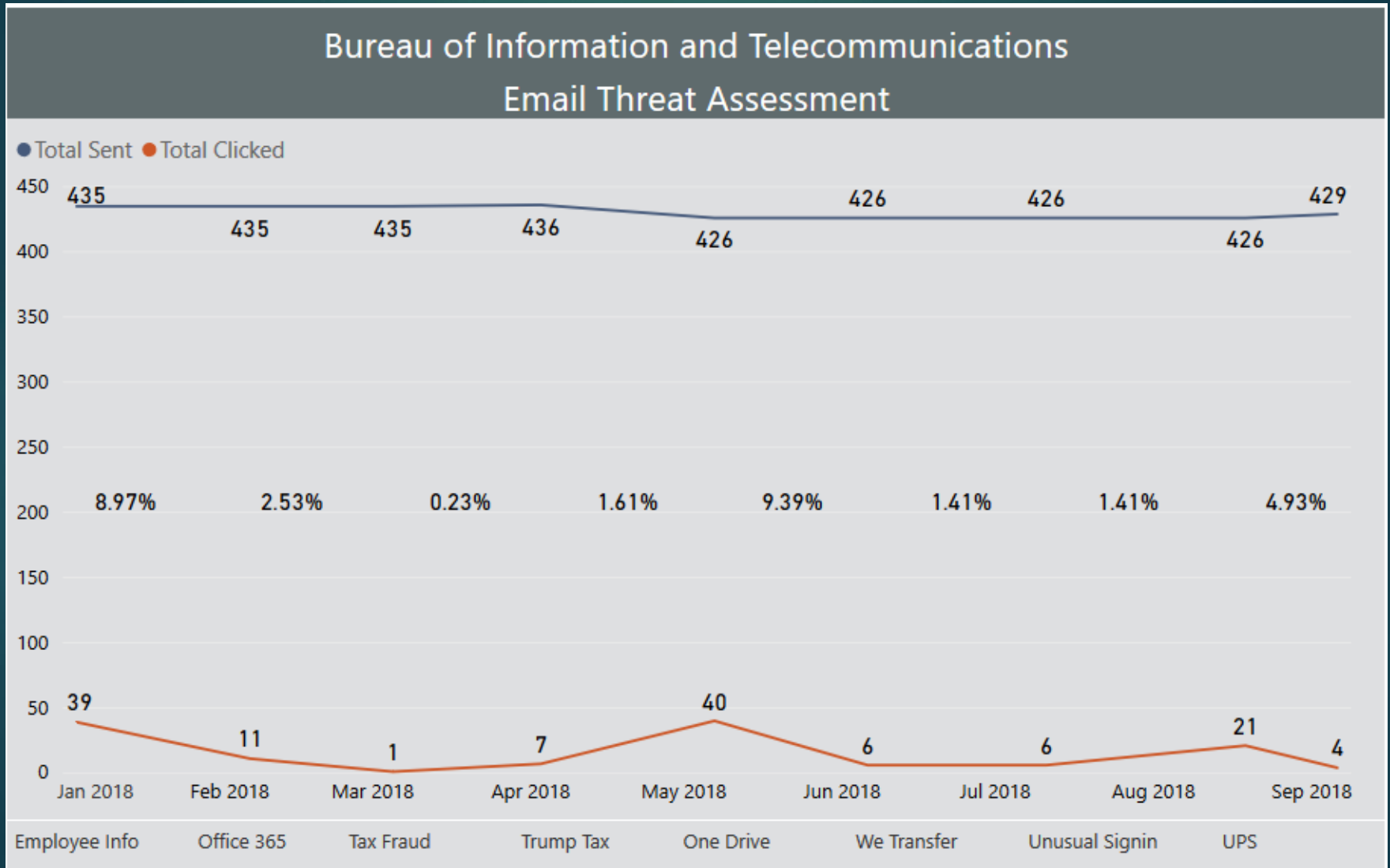
- Flexible
- Accessible
- Export Data
- Native Graphing – ok



1. Statewide Statistics

CampaignName	CampaignDate	Total Sent	Total Opened	Total Clicked	Click Percentage
Employees Verify Info	01/02/2018	7155	1048	1533	21.43%
Office 365	02/05/2018	7154	1041	399	5.58%
Tax Fraud	03/05/2018	7154	828	22	0.31%
Trump Tax	04/03/2018	7146	727	237	3.32%
One Drive	05/07/2018	7399	919	720	9.73%
We Transfer	06/06/2018	7399	935	448	6.05%
Unusual SignIn	07/11/2018	7399	1041	170	2.30%
UPS	08/19/2018	7529	939	723	9.60%
IT Alerts	09/06/2018	5022	659	127	2.53%
Total		63357	8137	4379	6.91%

2. Department View



Report: PowerBI

3. Individual Reporting

- All Failures
- Multiple Failures only

Email	Department	Status	CampaignName
john.doe@state.sd.us	Bureau of Information and Telecommunications	Clicked Link	Employees Verify Info
john.doe@state.sd.us	Bureau of Information and Telecommunications	Clicked Link	UPS
jake.doe@state.sd.us	Bureau of Information and Telecommunications	Clicked Link	We Transfer
jane.doe@state.sd.us	Bureau of Information and Telecommunications	Clicked Link	Employees Verify Info
jane.doe@state.sd.us	Bureau of Information and Telecommunications	Clicked Link	One Drive
ash.jones@state.sd.us	Bureau of Information and Telecommunications	Clicked Link	One Drive
ash.jones@state.sd.us	Bureau of Information and Telecommunications	Clicked Link	Unusual SignIn
amanda.smith@state.sd.us	Bureau of Information and Telecommunications	Clicked Link	One Drive
ben.franklin@state.sd.us	Bureau of Information and Telecommunications	Clicked Link	One Drive
bill.smith@state.sd.us	Bureau of Information and Telecommunications	Clicked Link	Office 365
will.iam@state.sd.us	Bureau of Information and Telecommunications	Clicked Link	Office 365
brendan.smith@state.sd.us	Bureau of Information and Telecommunications	Clicked Link	Employees Verify Info
brent.jones@state.sd.us	Bureau of Information and Telecommunications	Clicked Link	One Drive
smythe.smith@state.sd.us	Bureau of Information and Telecommunications	Clicked Link	One Drive
brett.abdul@state.sd.us	Bureau of Information and Telecommunications	Clicked Link	Employees Verify Info
adam.roof@state.sd.us	Bureau of Information and Telecommunications	Clicked Link	One Drive
koch.carter@state.sd.us	Bureau of Information and Telecommunications	Clicked Link	Employees Verify Info
nelson.mandela@state.sd.us	Bureau of Information and Telecommunications	Clicked Link	One Drive
carol.burnett@state.sd.us	Bureau of Information and Telecommunications	Clicked Link	Employees Verify Info
carol.burnett@state.sd.us	Bureau of Information and Telecommunications	Clicked Link	Unusual SignIn
shark.e@state.sd.us	Bureau of Information and Telecommunications	Clicked Link	Employees Verify Info
shark.e@state.sd.us	Bureau of Information and Telecommunications	Clicked Link	UPS

Report: E-mail Notification

- **2nd Failure**
 - Staff
 - Department Secretary

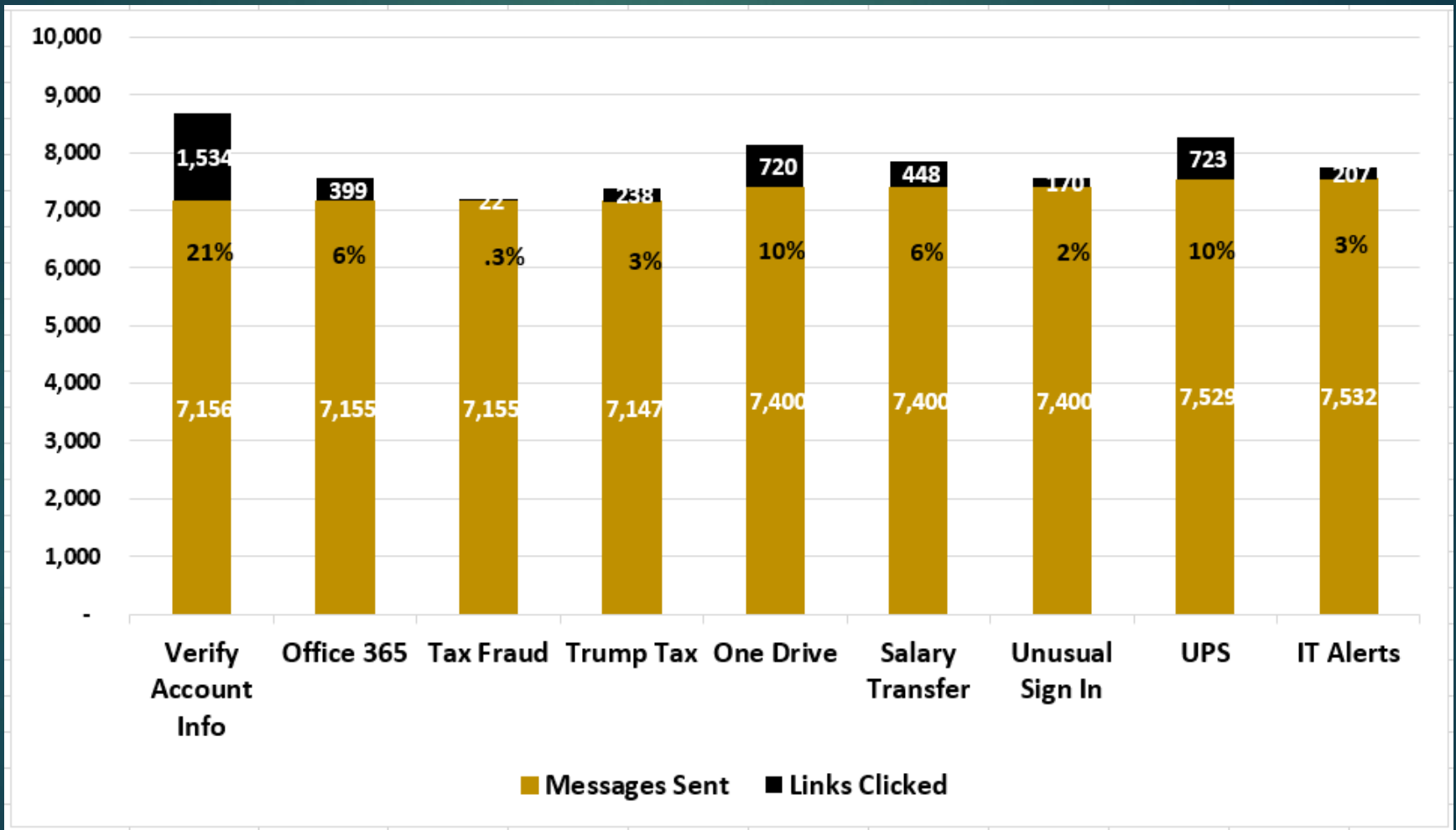
- **3rd Failure**
 - Staff
 - Department Secretary

- **4th Failure**
 - Points of Contact Meeting
 - Employee and supervisor
 - Options:
 - Multi Factor
 - Remove Software
 - Limit Access
 - ?

Report: In Person Training (3rd Phishing Failure)

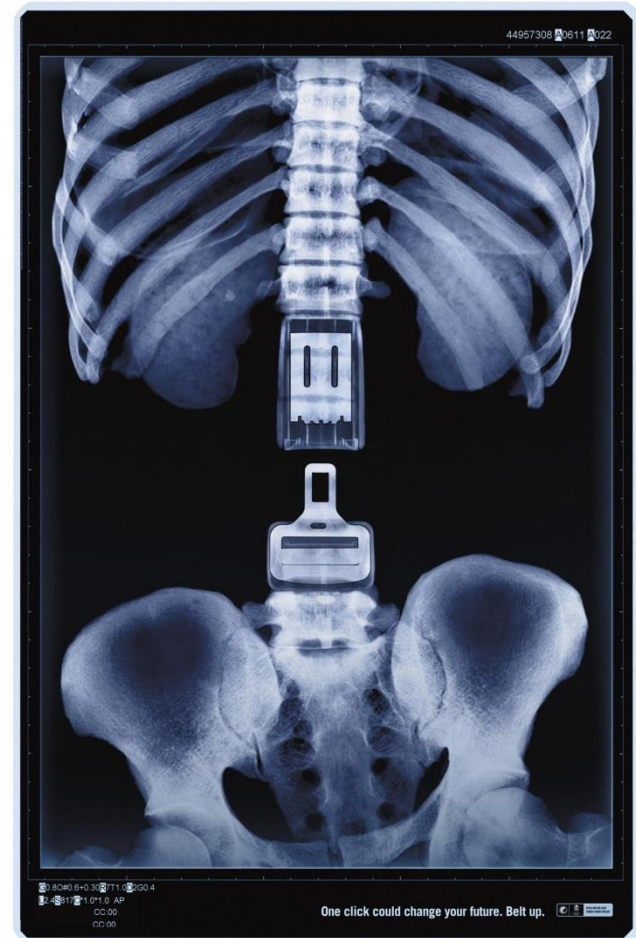
- 3 locations across the state
- Technologist Led
- ~1 hour
- 151 attendees YTD
- 38 4+

Email Threat Assessment Statewide: 2018



Lessons Learned

- Content is king
- Emotional Response
- Smartphones are a hindrance
- S L O W
D O W N



south dakota



bureau of
information &
telecommunications

Questions



Contact Information

Jim Edman

Deputy Commissioner and CISO
State of South Dakota
Jim.Edman@state.sd.us

Meredith Ward

Senior Policy Analyst
NASCIO
mward@NASCIO.org

Follow Us



@NASCIO



/NASCIOMedia



/NASCIOMedia



National Association of State
Chief Information Officers
(NASCIO)