Walleyes, Whales & Cybersecurity

October 2, 2018
SD State Government

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
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
BUREAU OF INFORMATION & TELECOMMUNICATIONS

FY 18

CYBER SECURITY SCOPE

- MOBILE DEVICES: 4,424
- VIRTUAL SERVERS: 1,023
- WAN SITES: 975
- DDoS ATTACKS: 74

- COMPUTERS & LAPTOPS: 8,981
- SERVERS: 228
- VOIP PHONES: 3,177

- BUSINESS APPLICATIONS: 1,094
- WEB GEO-BLOCKED ACCESS ATTEMPTS: 3,501,764
- MALWARE/VIRUS INFECTIONS: 1

- STATE FACILITATED PHISHING TESTS: 59,371
- SOFTWARE PACKAGES: 707
- MALICIOUS PHISHING EMAILS RECEIVED: 5,683

- PER YEAR
  - EMAILS PROCESSED: 132,581,015
  - EMAILS BLOCKED: 96,541,397 (73%)
  - EMAILS DELIVERED: 26,669,034
  - STATE FTE: 8,708
  - K12 ENROLLMENT: 132,520
  - BOR FTE: 5,154
  - HIGHER EDUCATION STUDENTS: 36,662
  - K12 TEACHERS & SUPPORT: 10,035

- CONTRACTS & AMENDMENTS: 183
- WEBSITES: 850
- INTERNET USAGE AVERAGE DATA TRANSMISSION / SECOND: 14.5 GBPS
- HACKSCANS: 33,646,000
- PETABYTES OF STORAGE: 1.46 PB

- COMPLETED AUDITS: 30
Cyber Infrastructure

- Perimeter Security
  - Authorized Use - Entities
  - Authorized Use - Citizens

- Network Security
- Endpoint Security
- Application Security
- Data Security

- Policy & Prevention
  - Awareness & Training
  - Architecture & Design
  - Risk Management & Audits

- Monitoring & Response
  - Incident Response
  - Forensics
  - Log Analysis & Management
  - SOC / NOC Monitoring 24x7
Problem:
Email Threat Assessment
January – September 2017
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):
  1\textsuperscript{st} Nothing
  2\textsuperscript{nd} Notification:
    - Individual
    - Department Head
  3\textsuperscript{rd} Attend In Person training
  4\textsuperscript{th} Account access review
## Cyber Security Training

**Statewide Completion:** 96%

<table>
<thead>
<tr>
<th>Agency</th>
<th>Completion Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>BFM</td>
<td>100.00%</td>
</tr>
<tr>
<td>BHR</td>
<td>100.00%</td>
</tr>
<tr>
<td>BIT</td>
<td>100.00%</td>
</tr>
<tr>
<td>DENR</td>
<td>100.00%</td>
</tr>
<tr>
<td>DLA</td>
<td>100.00%</td>
</tr>
<tr>
<td>DOM</td>
<td>100.00%</td>
</tr>
<tr>
<td>DOR</td>
<td>100.00%</td>
</tr>
<tr>
<td>DPS</td>
<td>100.00%</td>
</tr>
<tr>
<td>GOED</td>
<td>100.00%</td>
</tr>
<tr>
<td>LOT</td>
<td>100.00%</td>
</tr>
<tr>
<td>SDRS</td>
<td>100.00%</td>
</tr>
<tr>
<td>SIC</td>
<td>100.00%</td>
</tr>
<tr>
<td>SOS</td>
<td>100.00%</td>
</tr>
<tr>
<td>SPL</td>
<td>100.00%</td>
</tr>
<tr>
<td>Tribal</td>
<td>100.00%</td>
</tr>
<tr>
<td>DLR</td>
<td>99.88%</td>
</tr>
<tr>
<td>TOUR</td>
<td>98.61%</td>
</tr>
<tr>
<td>DOE</td>
<td>98.55%</td>
</tr>
<tr>
<td>GFP</td>
<td>98.47%</td>
</tr>
<tr>
<td>BOA</td>
<td>98.21%</td>
</tr>
<tr>
<td>PUC</td>
<td>96.67%</td>
</tr>
<tr>
<td>DOH</td>
<td>96.47%</td>
</tr>
<tr>
<td>ATG</td>
<td>95.45%</td>
</tr>
<tr>
<td>DSS</td>
<td>95.44%</td>
</tr>
<tr>
<td>GOV</td>
<td>94.74%</td>
</tr>
<tr>
<td>SDDOA</td>
<td>94.30%</td>
</tr>
<tr>
<td>DVA</td>
<td>94.29%</td>
</tr>
<tr>
<td>DHS</td>
<td>93.94%</td>
</tr>
<tr>
<td>AUD</td>
<td>93.75%</td>
</tr>
<tr>
<td>DOT</td>
<td>89.40%</td>
</tr>
<tr>
<td>DOC</td>
<td>89.22%</td>
</tr>
<tr>
<td>TREA</td>
<td>88.89%</td>
</tr>
</tbody>
</table>

*Statewide Avg: 95.70%*
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

Government Information <GovInfoSystem@state.sd.us>

EXT] All State Employees REQUIRED to verify info

To: Edman, Jim (EIT)

Retention Policy: Never Delete (Never)

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.

SDGOV

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.
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

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
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 South Dakota State Fair!

[Link to enter State ID]

Enter State ID Here
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

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.
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**

![Phishing Results 2018](image.png)
## 1. Statewide Statistics

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

2. Department View

Bureau of Information and Telecommunications
Email Threat Assessment

- Total Sent: 435, 435, 435, 436, 426, 426, 426, 426, 429
- Total Clicked: 8.97%, 2.53%, 0.23%, 1.61%, 9.39%, 1.41%, 1.41%, 4.93%

- Employee Info: 39, 11, 1, 7, 40, 6, 6, 21, 4
- Office 365: 0, 1, 0, 0, 0, 0, 0, 0, 0
- Tax Fraud: 0, 0, 0, 0, 0, 0, 0, 0, 0
- Trump Tax: 0, 0, 0, 0, 0, 0, 0, 0, 0
- One Drive: 0, 0, 0, 0, 0, 0, 0, 0, 0
- We Transfer: 0, 0, 0, 0, 0, 0, 0, 0, 0
- Unusual Signin: 0, 0, 0, 0, 0, 0, 0, 0, 0
- UPS: 0, 0, 0, 0, 0, 0, 0, 0, 0
3. Individual Reporting

- All Failures
- Multiple Failures only

<table>
<thead>
<tr>
<th>Email</th>
<th>Department</th>
<th>Status</th>
<th>Campaign Name</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:john.doe@state.sd.us">john.doe@state.sd.us</a></td>
<td>Bureau of Information and Telecommunications</td>
<td>Clicked Link</td>
<td>Employees Verify Info</td>
</tr>
<tr>
<td><a href="mailto:john.doe@state.sd.us">john.doe@state.sd.us</a></td>
<td>Bureau of Information and Telecommunications</td>
<td>Clicked Link</td>
<td>UPS</td>
</tr>
<tr>
<td><a href="mailto:jake.doe@state.sd.us">jake.doe@state.sd.us</a></td>
<td>Bureau of Information and Telecommunications</td>
<td>Clicked Link</td>
<td>We Transfer</td>
</tr>
<tr>
<td><a href="mailto:jane.doe@state.sd.us">jane.doe@state.sd.us</a></td>
<td>Bureau of Information and Telecommunications</td>
<td>Clicked Link</td>
<td>Employees Verify Info</td>
</tr>
<tr>
<td><a href="mailto:jane.doe@state.sd.us">jane.doe@state.sd.us</a></td>
<td>Bureau of Information and Telecommunications</td>
<td>Clicked Link</td>
<td>One Drive</td>
</tr>
<tr>
<td><a href="mailto:ash.jones@state.sd.us">ash.jones@state.sd.us</a></td>
<td>Bureau of Information and Telecommunications</td>
<td>Clicked Link</td>
<td>One Drive</td>
</tr>
<tr>
<td><a href="mailto:ash.jones@state.sd.us">ash.jones@state.sd.us</a></td>
<td>Bureau of Information and Telecommunications</td>
<td>Clicked Link</td>
<td>Unusual SignIn</td>
</tr>
<tr>
<td><a href="mailto:amanda.smith@state.sd.us">amanda.smith@state.sd.us</a></td>
<td>Bureau of Information and Telecommunications</td>
<td>Clicked Link</td>
<td>One Drive</td>
</tr>
<tr>
<td><a href="mailto:ben.franklin@state.sd.us">ben.franklin@state.sd.us</a></td>
<td>Bureau of Information and Telecommunications</td>
<td>Clicked Link</td>
<td>One Drive</td>
</tr>
<tr>
<td><a href="mailto:bill.smith@state.sd.us">bill.smith@state.sd.us</a></td>
<td>Bureau of Information and Telecommunications</td>
<td>Clicked Link</td>
<td>Office 365</td>
</tr>
<tr>
<td><a href="mailto:will.jam@state.sd.us">will.jam@state.sd.us</a></td>
<td>Bureau of Information and Telecommunications</td>
<td>Clicked Link</td>
<td>Office 365</td>
</tr>
<tr>
<td><a href="mailto:brendan.smith@state.sd.us">brendan.smith@state.sd.us</a></td>
<td>Bureau of Information and Telecommunications</td>
<td>Clicked Link</td>
<td>Employees Verify Info</td>
</tr>
<tr>
<td><a href="mailto:brent.jones@state.sd.us">brent.jones@state.sd.us</a></td>
<td>Bureau of Information and Telecommunications</td>
<td>Clicked Link</td>
<td>One Drive</td>
</tr>
<tr>
<td><a href="mailto:smythe.smith@state.sd.us">smythe.smith@state.sd.us</a></td>
<td>Bureau of Information and Telecommunications</td>
<td>Clicked Link</td>
<td>One Drive</td>
</tr>
<tr>
<td><a href="mailto:brett.abdul@state.sd.us">brett.abdul@state.sd.us</a></td>
<td>Bureau of Information and Telecommunications</td>
<td>Clicked Link</td>
<td>Employees Verify Info</td>
</tr>
<tr>
<td><a href="mailto:adam.roof@state.sd.us">adam.roof@state.sd.us</a></td>
<td>Bureau of Information and Telecommunications</td>
<td>Clicked Link</td>
<td>One Drive</td>
</tr>
<tr>
<td><a href="mailto:koch.carter@state.sd.us">koch.carter@state.sd.us</a></td>
<td>Bureau of Information and Telecommunications</td>
<td>Clicked Link</td>
<td>Employees Verify Info</td>
</tr>
<tr>
<td><a href="mailto:nelson.mandela@state.sd.us">nelson.mandela@state.sd.us</a></td>
<td>Bureau of Information and Telecommunications</td>
<td>Clicked Link</td>
<td>One Drive</td>
</tr>
<tr>
<td><a href="mailto:carol.burnett@state.sd.us">carol.burnett@state.sd.us</a></td>
<td>Bureau of Information and Telecommunications</td>
<td>Clicked Link</td>
<td>Employees Verify Info</td>
</tr>
<tr>
<td><a href="mailto:carol.burnett@state.sd.us">carol.burnett@state.sd.us</a></td>
<td>Bureau of Information and Telecommunications</td>
<td>Clicked Link</td>
<td>Employees Verify Info</td>
</tr>
<tr>
<td><a href="mailto:shark.e@state.sd.us">shark.e@state.sd.us</a></td>
<td>Bureau of Information and Telecommunications</td>
<td>Clicked Link</td>
<td>UPS</td>
</tr>
<tr>
<td><a href="mailto:shark.e@state.sd.us">shark.e@state.sd.us</a></td>
<td>Bureau of Information and Telecommunications</td>
<td>Clicked Link</td>
<td>Employees Verify Info</td>
</tr>
</tbody>
</table>
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

- Verify Account Info: 1,534 (21%) Messages Sent, 1,534 (21%) Links Clicked
- Office 365: 399 (6%) Messages Sent, 399 (6%) Links Clicked
- Tax Fraud: 22 (0.3%) Messages Sent, 22 (0.3%) Links Clicked
- Trump Tax: 258 (3%) Messages Sent, 258 (3%) Links Clicked
- One Drive: 720 (10%) Messages Sent, 720 (10%) Links Clicked
- Salary Transfer: 448 (6%) Messages Sent, 448 (6%) Links Clicked
- Unusual Sign In: 170 (2%) Messages Sent, 170 (2%) Links Clicked
- UPS: 723 (10%) Messages Sent, 723 (10%) Links Clicked
- IT Alerts: 7,532 (3%) Messages Sent, 7,532 (3%) Links Clicked
Lessons Learned

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