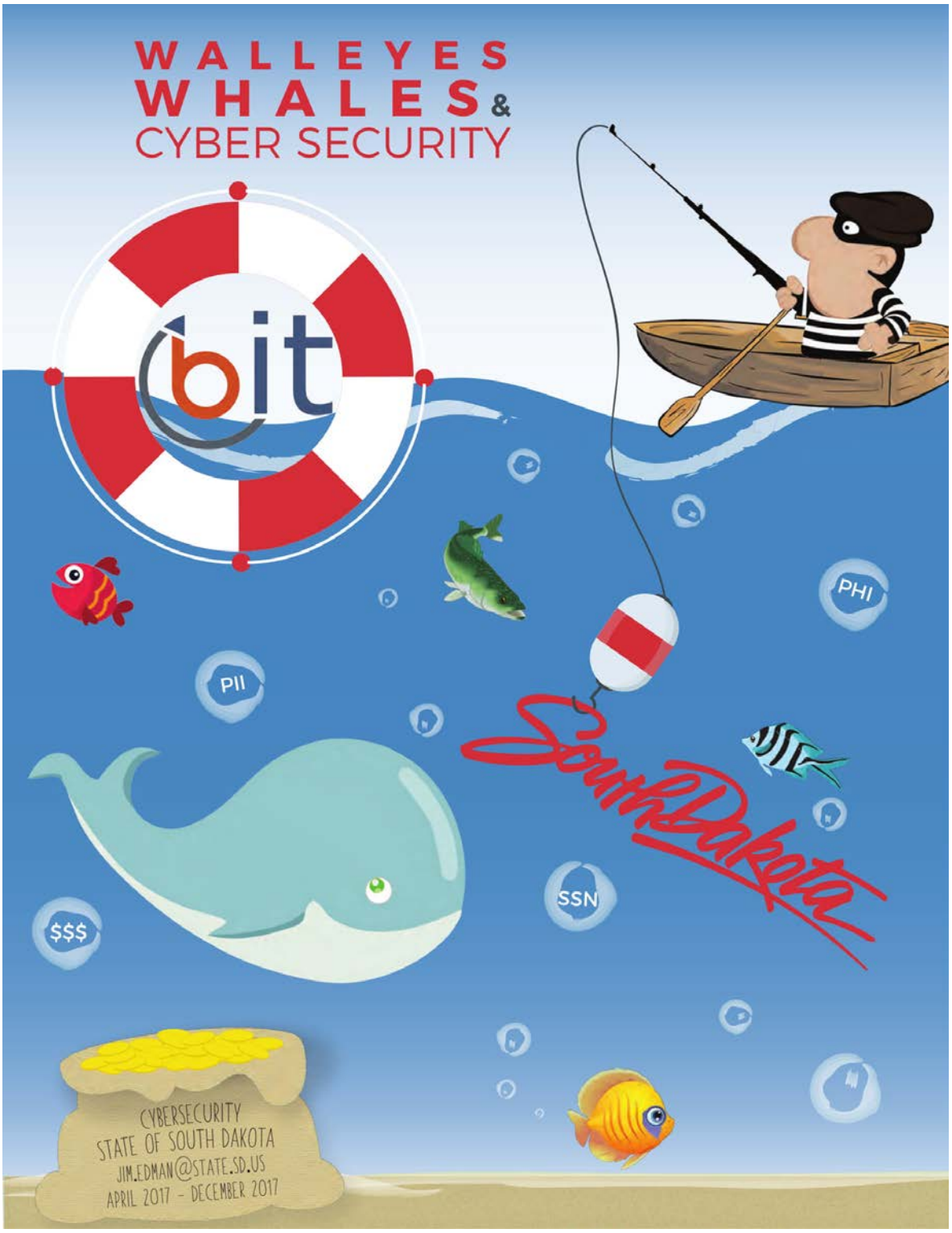

WALLEYES
WHALES &
CYBER SECURITY
bit
PHI
PII
SSN
$$$
SouthDakota
CYBERSECURITY
STATE OF SOUTH DAKOTA
JIM.EDMAN@STATE.SD.US
APRIL 2017 - DECEMBER 2017

Walleyes Whales & Cybersecurity

Executive Summary

The walleye is South Dakota's state fish. The opportunity to catch this delicious and challenging sport fish draws many South Dakotans and tourists to the clear, blue waters across the state. This form of fishing is a great sport that brings significant quality of life advantages to the Upper Plains. Email phishing on the other hand is akin to the silver (flying) carp of the fishing variety. In the best-case scenario, it is a nuisance, worst case it is very dangerous. Protecting our staff and elected officials (i.e. the whales) from the threatening aspects of email phishing is the basis for our program. There are many areas of protection required to safeguard government data and protection from the email attack vector is of paramount importance.

Industry measures highlight the magnitude of the email risk. According to the 2018 Verizon Data Breach Investigations Report, *Phishing and pretexting represent 98% of social incidents and 93% of breaches. Email continues to be the most common vector (96%).*

Building on that statistic, the Symantec Internet Security Threat Report indicates that "*The highest rate of email-borne malware was for organizations in the Public Administration sector.*" 1 in every 120 emails delivered to the Public Administration sector was laced with malware.

These statistics reinforce what is common knowledge to those of us in the government technology sector. If phishing is not the greatest, it is certainly one of top risks to cybersecurity within state government.

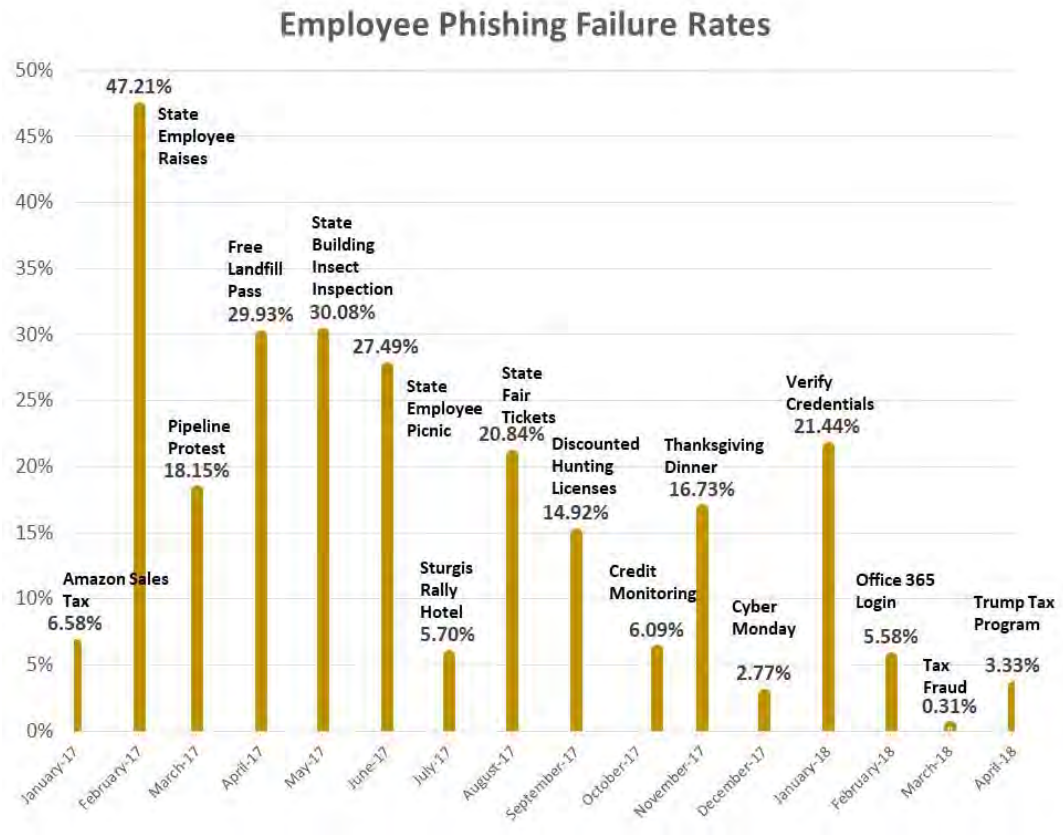
To combat this risk, South Dakota takes an aggressive approach to education, assessment, and establishing expectations. Government employees have broad access to sensitive information. Cybersecurity in general applies defense-in-depth principles including many overlapping layers. Protecting ourselves from the phishing attack vector is a critical aspect of our defense.

The concept for our assessments began in early 2017 as we recognized far too many failures from our internal testing. (See page 3). We initiated our own phishing testing to assess the degree of knowledge within the staff. The early findings were surprising. The lifecycle of the project began with the discovery of the problem, building of the policy, establishing the service, enhancing of the education efforts, building of the videos and training themes, the reporting of the results through active analysis and finally the communications of the results to staff and senior management.

An educated staff is an essential asset in the reduction of cybersecurity risk. Our goal in the service is to change the decision-making process on whether to click on a link or attachment from a content-driven or emotional decision to an educated and informed strategy. The progress shown on the graph in 2018 demonstrates we have turned the corner in our awareness and education.

Impact

The following graph summarizes the problem, progress and impact of our service. Significant failure rates early led to revamping the service and improving our education efforts. Those failures were a key indicator that our previous education and trainings were not effective. We determined that establishing policy was needed to legitimize our efforts. We also identified our analysis and reporting processes needed considerable enhancements beyond a simple, raw failure rate. Specific departmental and individual level reporting was required.



The bars above show the failure percentage along with the phishing topic. The graph suggests employee curiosity about a message's content easily overrides employee caution. Those topics with a high emotional interest most frequently resulted in employees clicking on a link or attachment within the message. The topic of employee raises with a failure of 47% is shocking. 'Free passes' up to 30% failures are indicative of the emotional reactions. This taught us that we needed to improve our training towards our ~7,000 state employees. As the failure trend continues to decrease, the overall risk management posture for this attack vector is diminished. Though it may not disappear, being able to manage a smaller magnitude of risk is attainable.

Limited financial resources steered us to using publicly available resources in combination with in-house expertise. We built our own phishing methodology using open source software. Commercial products were evaluated, but the return on investment for the off-the-shelf products compared to the open source tools was not justified. The estimate provided for the leading industry product was a $105,000 for three years. Our self-built tools and process cost less than $5,000 in staff time to establish.

Concept

The program is based on four tenets:

A. Policy – establishing the oversight and expectations.
B. Training – continuous cycle to educate staff.
C. Assessment – continuous evaluation of staff knowledge.
D. Analysis – continuous review of progress and setbacks of the service.

A. Policy

The first step in the phishing service is the establishment of expectations in policy. The Bureau of Human Resources established the Cybersecurity Awareness Assessment Policy in late 2017 with BIT input. The intent of the policy is to elevate the importance of information technology security and to clearly identify expected behavior of state employees. If successful, this will establish a culture of improved cybersecurity hygiene and responsibility. The policy includes expectations for training, reporting situations and consequences for not meeting cybersecurity best practice behaviors. A summary of the policy follows:

1) Each employee shall successfully complete annual cybersecurity training.
2) Employees have the responsibility to recognize and report suspicious situations; if you see something, say something.
3) An employee who loses state technology assets (i.e. a laptop computer) or sensitive state data must notify the employee's supervisor and the BIT Help Desk immediately.
4) At least annually, BIT will test each employee with a cyber awareness exercise.
    a. An employee initially failing a security awareness assessment will be directed to an educational tutorial explaining how the employee should have identified the situation as a potential threat to the State's system. The employee will be subject to an additional assessment during the subsequent months.
    b. A second failure, in addition to a. will include the employee being contacted by a BIT employee who will explain the importance of cybersecurity and suggest how the employee may identify these risks. The employee's supervisor will be notified that the employee failed a second security awareness assessment.
    c. A third failure includes a. and b. plus the employee will be required to attend on-site cybersecurity training presented by BIT.
    d. A fourth failure includes a. b. c. and may be subject to disciplinary action.

B. Training

We have used multiple approaches to achieve educational success. Recognizing phishing and other malicious email can be learned by following a series of steps. New employees take our course within the first week of employment. The course topics include password management, identity theft, social engineering, physical security, travel safety, mobile data, privacy, and acceptable use. Additionally, specific classes towards phishing, federal tax information, and the Health Insurance Portability and Accountability Act are delivered to individuals depending on their responsibilities.

Course content is delivered online with tests following each chapter. A score of at least 70% is required to pass the chapter.

Employees are encouraged to submit suspicious phone calls, portable media, spam or phishing emails to our Help Desk. All items are then interrogated for risk. Employees submitting

dangerous requests may receive assorted items of 'goodwill' from the security group. This is in recognition of their good cybersecurity habits!

As part of Cybersecurity Month, additional training was offered to employees through a video produced by South Dakota Public Broadcasting and Lt. Governor Matt Michels. Utilizing the Lt. Governor's fantastic sense of humor, the video highlighted common phishing tricks in a skit purporting to be from the Lt. Governor's phantom Presidential campaign.

Finally, additional training is provided through our Assessment process detailed below.

C. Assessment

The assessment aspect of the program focuses on testing employee's grasp of the training through regular internal phishing tests. Though the policy gives us the opportunity to test employees yearly, we exercise the flexibility to test everyone monthly.

Preparation of phishing message

Our process begins with the monthly ingesting of our global address list. This ensures that the most recent set of email addresses is used. Resignations, retirements, and new hires make this a dynamic list. Next, that list is culled and all service accounts and public folders are removed. The remaining accounts are randomized and divided into groups of three. Each group is between 2,000 – 3,000 email addresses. This is our weekly target list. We have included all employees to generate the largest survey pool possible. Instead of a random subset of staff, we want the most precise empirical data possible.

Content Development of phishing message

As evidenced by our graph on Page 3, the content of the phishing email was the key factor in determining whether someone clicked on the email's link or attachment. This program improved the training to recognize phishing triggers and eliminate the 'curiosity factor'. We need to replace that immediate, emotional reaction with an orderly review of the clues present in the email.

The content we include in the assessment messages is driven by current news events, legislative activities, and other issues relevant for South Dakota. We also gather real phishing emails received by state employees and build off their design. The intent when picking a topic is to make it as realistic and emotive as possible. That's how the bad actors operate and our goal is to mimic their behavior.

The process begins with a theme or subject for our test email. An email message is created including text and graphics using publicly available information. The next step is key and includes building an educational video based on the email message. We find this to be a critical aspect of our education curriculum. The video includes text and audio descriptions of the triggers identifying what the client should have recognized as being suspicious in the email. The brief, two-minute video is customized for each campaign. It is important that the video is short and direct. We want employees to spot the exact suspicious components of the email they just received and to learn how to piece the various phishing hints together. The final creation step is

the combining of text, graphics, and a 'malicious' landing page or attachment into a phishing email.

The resulting messages are sent to one of the groups identified in the Preparation step. Phishing emails are delivered on random days the first three weeks of the month. If an employee clicks on a link within the email, it is recorded in a database and the education video is automatically launched.

D. Analysis

The analysis portion of the process is critical. Understanding where our risks lie and where improvements are needed allows us to continuously reduce our risk exposure from this vector. It was this type of qualitative analysis in 2017 that led us to the conclusion that our employees were woefully under educated on phishing.

The clicking results are exported daily into a database which is linked into our PowerBI analysis tool. PowerBI is used for various perspectives on viewing the data. Initially, you can see we get an overall perspective on the campaign failure rate.

CampaignName	Campaign Date	CampaignDescription	Total Sent	Total Opened	Total Clicked	Click Percent
Employees Verify Info	01/02/2018		7156	1048	1534	21.4
Office 365	02/05/2018		7155	1041	399	5.5
Tax Fraud	03/05/2018		7155	828	22	0.3
Trump Tax	04/03/2018		7147	727	238	3.3
One Drive	05/07/2018		4933	610	483	9.7
Total			**33546**	**4254**	**2676**	**7.9**

Next, we drill into the agency list to determine if some agencies are more susceptible than others. This is a subset of our agency reporting.

Department	Total Sent	Click Percentage	Total Clicked
School and Public Lands	29	24.14 %	7
Department of the Military	46	21.74 %	10
Department of Veteran Affairs	605	13.88 %	84
Department of Corrections	1756	12.02 %	211
Secretary of State	172	10.47 %	18
Department of Health	2847	9.87 %	281

Finally, we review specific departments and individuals. This is a critical step and includes the enforcement aspect of the Human Resources policy. Item 4) of the policy on Page 4 outlines the additional training required for individuals that fail the tests. The training is cumulative as each successive test is failed. Again, the goal is to increase the literacy of employees to better recognize the tricks used in phishing messages.

We have covered many of the important items in the program but we have accountability remaining as a key aspect. Accountability adds individual responsibility to each employee. Employees are answerable for their performance. The first failure for an individual result in him/her being directed to a video pertinent to the phishing campaign explaining the triggers present in the message. Our experience is that a multi-media message is more instructional

than a document, website or graphic. https://youtu.be/sZiWeCjv29g The second failure adds a contact from a technologist further explaining the phishing indicators. The employee's supervisor is also contacted notifying them of the failure. Finally, an in-depth video is also available reinforcing the curriculum of phishing considerations already covered. https://youtu.be/bjXUkrIYkbE

Monthly, the senior-most executive of a department receives a report. The report lists employees who have failed the phishing tests two or more times. This reporting incentivizes the department executive to stay current on the performance of their office. Additionally, an executive report comparing the performance of agencies against each other generates competition amongst the agencies to minimize their phishing failures. On top of the training provided previously, three failures include a requirement to attend a one-hour class in person further detailing the risks of cybersecurity and email hygiene. Failures four and above can invoke a wide range of personnel action, including loss of computer access through employment termination.

Significance

The scope of our trainings and assessments include nearly every aspect of government. Existing Executive Branch employees are required to take a one-hour course on cybersecurity annually to achieve 1) in the above Policy. Constitutional Offices along with the Unified Judicial System also participate on a voluntary basis. Our long-term partnership with those independent branches of government fuels their participation in our program, demonstrating their commitment to cyber security. In our consolidated IT environment, cyber security IS statewide from the desktop computer through networking with applications and data center integrated.

The uniqueness of Walleyes and Whales is that it is comprehensive. The policy is published, training is provided, assessment and follow-up education is performed in multiple ways, analysis is empirically-based and accountability is defined with known expectations and consequences. Many states perform internal email phishing, very few, if any, cover the depth defined here.

State CIO's have annually rated Security their Top Priority since 2014. That rating is a testament to the program's precedence. Cybersecurity professionals understand that a defense-in-depth strategy is based on a combination of technical and human tactics. Historically, we have spent an inordinate amount of our time on the technology segment. The results of our email phishing assessments have proven the human aspect is equally important. Changing human behavior is a complex process but progress is evident. Our goal with Walleyes and Whales is to continuously educate and assess employees on the tricks used by bad actors to help them counter our natural emotion-based reactions. Cybersecurity is a process, not a singular step. Providing employees creative and relevant training with immediate feedback is a significant step in that process of protecting the confidential data we are entrusted to safeguard.