DEVELOPING KEY SECURITY RISK INDICATORS THROUGH CYBER ANALYTICS AND CORRELATION

NOMINATING CATEGORY:

CYBERSECURITY

NOMINATOR:

JOHN MACMILLAN,
CHIEF INFORMATION OFFICER

COMMONWEALTH OF PENNSYLVANIA
1 TECHNOLOGY PARK
HARRISBURG, PA 17110
717-772-8013
JMACMILLAN@PA.GOV

INITIATION: FEBRUARY 2019

COMPLETION: DECEMBER 2019

EXECUTIVE SUMMARY:

Inherent within the “defense in depth” tenet of cybersecurity is the existence of multiple and ongoing efforts to adapt and strengthen the security posture of the organization, as well as a need to evaluate the effectiveness of each effort, not only on its own merit, but also in light of how it interacts with or affects the success of other cybersecurity efforts. However, the data reflecting the outcomes and related metrics from these efforts are often disparate in nature, making cross-effort correlations difficult.

The Commonwealth of Pennsylvania, Governor’s Office of Administration, Enterprise Information Security Office (EISO) has undertaken an effort to tackle these challenges and to provide management-level views into the effectiveness of its programs and their inter-relationship with each other.

For some time now, the Pennsylvania has used data dashboards to provide real-time views into its security incident management system. These views provide insight into the overall status of tickets, their distribution in terms of severity, and their distribution across IT service delivery groups and state agencies. These real-time views have already proven themselves valuable by creating efficiency improvements in the generation of monthly and quarterly executive reports.

Recently, Pennsylvania has focused on correlating this data with other efforts outside of the security incident management system, including:

- Completion of the annual security awareness end user training, IT administrator training, and other required training
- Results of phishing exercises conducted with employees
- Privileged users or those with other elevated access rights

As a result of this work, Pennsylvania has been able to more effectively target its training campaigns to appropriate segments of the workforce, adjust the content of trainings to make them more meaningful to the target audiences, and better prioritize its efforts in incident management. As a result, more employees are recognizing potential phishing emails, as demonstrated through exercises, and a new process was implemented to reduce inactive contractor accounts.

Based on the success of this effort, Pennsylvania is moving forward and expanding the program to include Application Security and Enterprise Risk Analysis to better secure applications and systems across the enterprise and protect the assets in an effective, prioritized manner.

CONCEPT

Cybersecurity technologies and program work streams produce large volumes of data. While useful, on their own, these data streams do not always paint a comprehensive picture of risk or targeted opportunities for financial investment in cybersecurity. However, when these independent work streams and sources are correlated together, they can provide valuable and measurable visual insights that help to articulate risk comprehensively across a given area, and help realize opportunities for cybersecurity financial and resource investments, that may have otherwise gone unnoticed.

The Pennsylvania Office for Administration's (OA) Enterprise Information Security Office (EISO) embarked on a cyber analytics project to provide deeper insights on risks and trends on various topics. The project focused on analyzing and correlating large volumes of disparate data to develop Key Security Risk Indicators to measure different types of risk and opportunities for cyber security investment. The first area of focus for the initiative project was training.

Security awareness training empowers our workforce with the knowledge they need to recognize and report potential cyber threats. Like all organizations, EISO strives to achieve 100% training coverage, and has established an innovative method converging several independent efforts. As part of Pennsylvania's security awareness campaigns, EISO conducts periodic phishing tests not just as an outcome of the periodic training, but also to identify segments of the workforce that require additional training.

Through an analysis of recent malware attacks, EISO identified that attacks on users with elevated privileges are most often responsible for unauthorized access to sensitive agency information. Hence, a need to reduce the number of users with elevated access and additional training.

On their own, each of these measurements depicts a facet of end user risk, but only tells one part of a greater story. Once the data is correlated together, with the ability to visualize and view the data in different dimensions, a more comprehensive view of end user risk emerges.

Using the insights gained from the correlation of these data, Pennsylvania identified opportunities to prioritize actions related to:

1. Employees and contractors with user privileges who fall prey to phishing exercises and have not taken awareness training
2. Employees and contractors with elevated privileges (with system account access) who fall prey to phishing exercises and have not taken awareness training
3. The effectiveness of the computer-based training course and learning objectives.

Figure 1 reflects the correlation between the rate of privileged users who have not completed their training with the rate at which those uses clicked links in a phishing test.

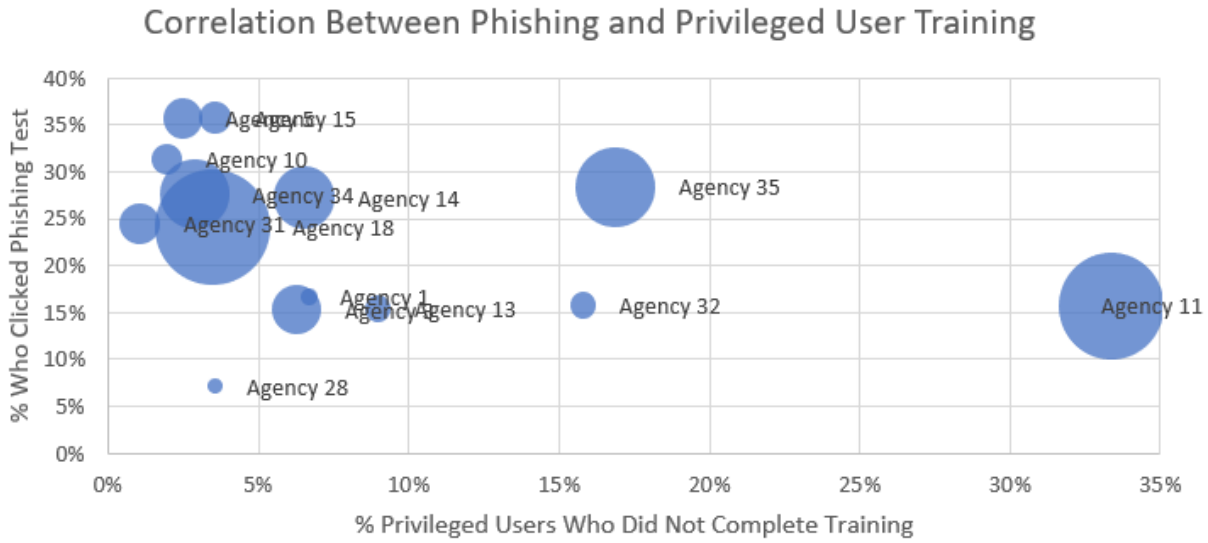

Figure 1 - Correlation Phishing and Privileged User Training (bubble size reflects # of privileged users in the agency)

Despite most of the users having completed of their training (low non-completion rate), about 25% of these privileged used failed to identify a targeted phishing email and proceeded to click on the embedded “malicious” link it contained.

In response, we have reviewed our training materials to make them more effective. A more recent test, reflecting the success of this effort, can be seen in Figure 2. This figure reflects a high training completion rate (~95%) along with a correspondingly low click rate (~4%) in phishing test for the overall Commonwealth workforce.

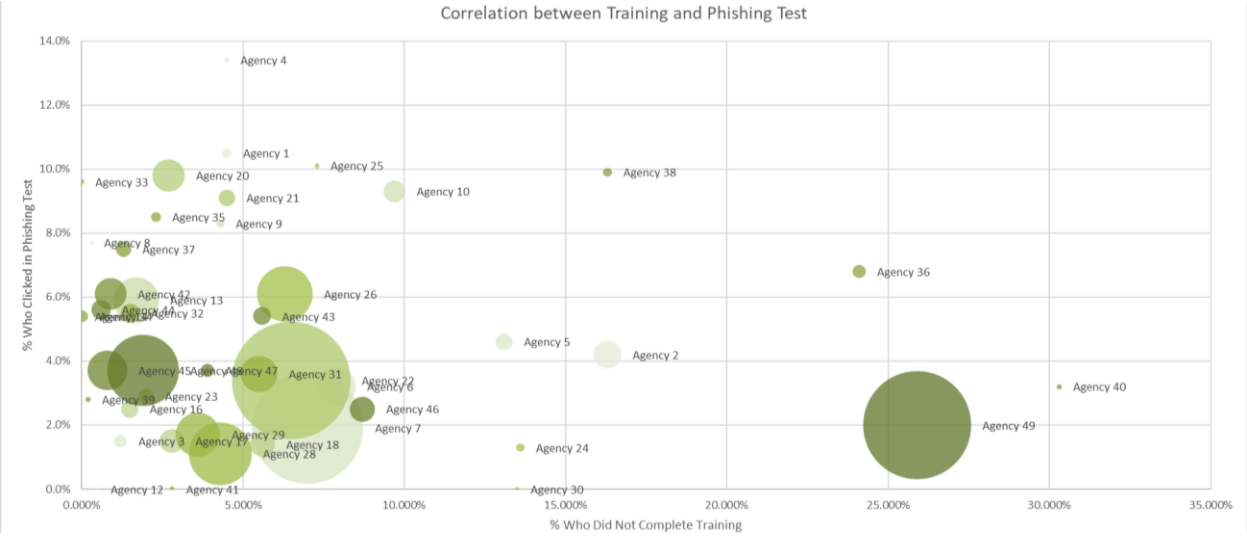

Figure 2- Correlation Between Training and Phishing (bubble size reflects agency population)

Figure 3 shows the correlation between completion of the security awareness training with different segments of the workforce. Completion of the training by employees is about 94% whereas for contractors it is only around 59%. After conducting further research, EISO discovered various factors contributing to the low completion rate. One significant factor was the failure of timely off-boarding of contractors once their work was completed. This has resulted in a new automated process to offboard inactive contractors. Since its initiation early in May, 2020, over 1,200 such contractor accounts have been purged from the system, thereby reducing the risk of "orphan" accounts being exploited to conduct attacks.

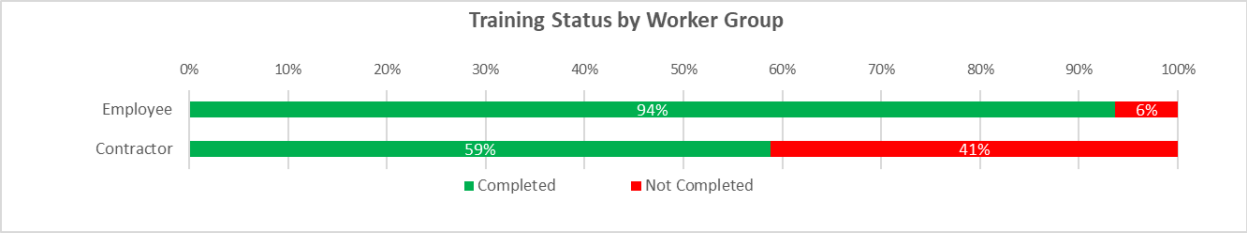

Figure 3 - Security Awareness Training Completion by Workforce

As a final example, to help prepare for 2020 election, EISO has conducted targeted phishing exercises for elections workers in the PA Department of State. The goal is to reinforce the training these workers have taken. Figure 4 reflect the success we have had in meeting this goal with a consistent downward trend over time.

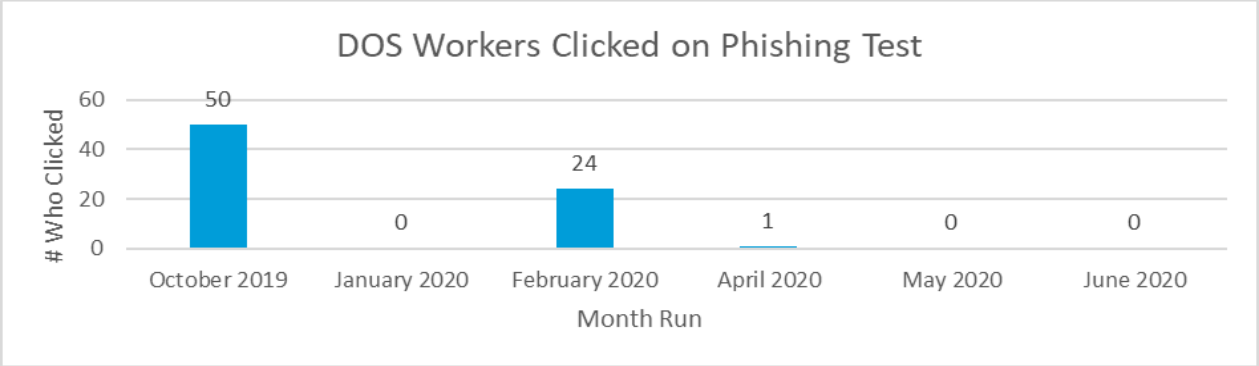

Figure 4 - Effectiveness of Training and Phishing Testing for Department of State

These correlation outcomes enabled Pennsylvania to prioritize end-user risk and perform a targeted campaign to enforce training completion. Privileged access was removed or reduced until additional trainings were completed and automated contractor account remediation has been put into place.

Building on our success with the correlated analytics for training and security awareness metrics, EISO is looking to expand its use of cyber analytics to address additional business needs, such as correlation of vulnerability and threat data, and risk assessment and mitigation.

Going forward, the cyber analytics program will be expanded to include integrated analysis and reporting for ongoing cyber risks. As illustrated in Figure 5, this expanded platform will contain three core components:

1. Risk Register for risk intake, consolidation and mitigation planning.
2. Security Information and Events Monitoring (SIEM) for ingesting system logs and identifying anomalies.
3. Cyber Analytics for correlating disparate data and high data volumes.

Each of these components will tie into our Training and Configuration/Asset systems to provide agency stakeholders and executive management a comprehensive, near real time view of our cybersecurity posture.

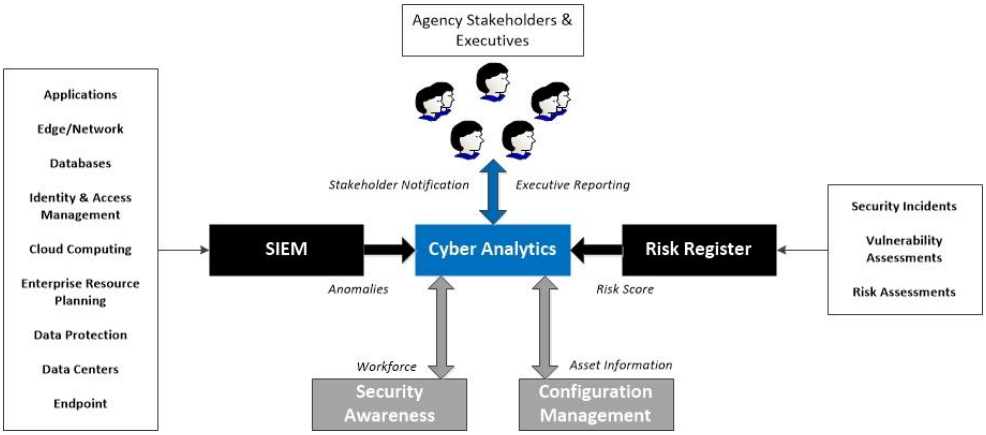

Figure 5 - Correlation of Risk with Cyber Analytics

This will enable the EISO to better and collaboratively balance cybersecurity and business needs with our agency partners such as:

Application Security:
Agencies perform periodic vulnerability scans to identify and mitigate system misconfigurations. By correlating the scan results with external alerts and trends, the EISO will be able to quickly identify emerging threats to enable early mitigation strategy.

Enterprise Risk Analysis:
EISO performs periodic risk assessments to establish consistent and appropriate safeguards. These risks are generally identified and mitigated at the agency level. By correlating these risk findings across several agencies, available safeguards and mitigation plans, the EISO will be better able to better guide risk and financial/budget conversations with other stakeholders.

SIGNIFICANCE

The success of the correlated analytics effort has enabled EISO to embark on additional initiatives to elevate visibility, prioritize actions, and target specific user groups as needed. The project aligns with two of NASCIO's Top 10 State CIO Priorities: #1 Cybersecurity and Risk Management and #8 Data Management and Analytics. It also aligns to the Pennsylvania CIO's goals and strategies to 1) optimize services through enhanced cybersecurity capabilities, and 2) foster collaboration, communication and governance through increased business risk awareness and actions to mitigate.

The project demonstrates how advance data analysis techniques can elevate performance metrics to the next level to identify previously unknown needs and target investments to address them. Pennsylvania's commitment to data-driven decision-making is yielding better outcomes for citizens and more effective utilization of financial and staffing resources dedicated to cybersecurity.

IMPACT

The EISO's ability to correlate security outcomes from disparate sources such as:

- Security Awareness Training, the IT Administrator Training, and other required training;
- phishing exercises; and
- privileged users or those with other elevated access rights

with incident and other metrics has enabled Pennsylvania to:

- More effectively target its training campaigns to appropriate communities
- Adjust the content of that training to make it more meaningful to its audience
- Better prioritize its efforts in incident management.

These correlation outcomes enabled Pennsylvania to prioritize end-user risk and perform a targeted campaign to enforce awareness training completion. Privileged access was removed or reduced until additional trainings were completed. Automated contractor account remediation has been put into place with the deactivation of over 1,200 inactive accounts since as of May. These risk reduction efforts have led to measurable improvements as seen in the figures above including higher completion rates for training and improved performance by users in phishing exercises.

Moving forward, additional datasets for measuring other areas of risk are being integrated such as correlation of vulnerability and threat data, and, risk assessment and mitigation.

Expanding the program to include Application Security and Enterprise Risk Analysis will further enable Pennsylvania to better secure its applications and systems across the enterprise and protect those assets in an effective, prioritized manner.