ENHANCING COLLABORATION ACROSS STATE AND LOCAL GOVERNMENT TO IMPROVE CYBERSECURITY OUTCOMES FOR EVERYONE

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 2020

EXECUTIVE SUMMARY:

Pennsylvania is home to 67 counties, over 2,500 municipalities and 500 school districts. These numerous political subdivisions run the gamut from rural areas with small populations to large cities such as Pittsburgh and Philadelphia. Correspondingly, the human and financial resources available to them vary greatly. As a result, there is a great disparity in cybersecurity capabilities across our counties and other areas of local government, amounting to cases of *haves* and *have-nots*.

As in many other states, counties are tasked with conducting local, statewide and national elections. Counties also serve as the point of contact for other public services and programs, many of which require the exchange of data with state agencies and/or interaction between local and state IT systems. Due to the interconnected nature of many state and local agencies, the disparities we see and the presence of *haves* and *have-nots* must be addressed to provide a strong cybersecurity defense for elections and other government services.

To strengthen overall election security in Pennsylvania and to further our mission to mature the commonwealth's overall cybersecurity posture, the Office of Administration (OA) is working closely with the County Commissioners Association of Pennsylvania (CCAP) to provide cybersecurity programs and other shared services and has begun to forge similar partnerships with school districts and cities.

Through its partnership with CCAP, OA leveraged the commonwealth's buying power to achieve economies of scale in the purchase of licenses for a 3rd party security training and testing service, as well as provided copies of its own security awareness training materials. Today, each county has its own tenant in the service that is not shared by the other counties or by the commonwealth. This initiative helps to bolster security, aligns with best practices, and has achieved economies of scale, reduction of overall costs, maximized efficiencies, increased knowledge transfer, reduced duplication of work and streamlined processes and services. CCAP and the counties have reported favorably on the program and it will be renewed for the upcoming fiscal year.

OA undertook another program to provide each county with memberships to the Multi-State Information Sharing and Analysis Center (MS-ISAC) and the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) to provide access to additional resources to support cyber defense, including sector-specific threat intelligence products, incident response and remediation, threat and vulnerability monitoring, cybersecurity awareness and training products and tools for implementing security best practices. As a second phase of the program, OA and the PA Department of State (DOS) collaborated with MS-ISAC and CCAP to deploy Albert Sensors to each county. The Albert program is an Intrusion Detection System (IDS) that provides 24x7 monitoring of the sensors and notifications of potential malicious activity. Already, sensors have been deployed to almost 2/3 of the 67 counties.

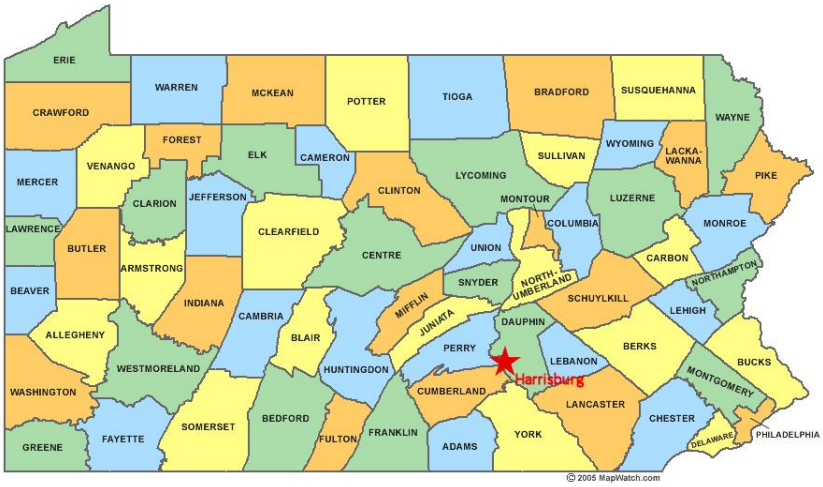
Commonwealth-wide, the coordinated training initiative has realized up to 50% in cost savings compared to the counties and commonwealth procuring services individually. From a business value perspective, this has resulted in net return on security investment (ROSI) of $1,344,000.

Due to the overwhelming success of this standardized shared services approach, OA is expanding its collaborative umbrella to other areas of local and state government including the four caucuses of the Pennsylvania General Assembly, school districts, cities and higher education. The approach taken in

Pennsylvania recognizes the common challenges and opportunities shared by state and local governments in cybersecurity and provides a model for other states to emulate with their local partners for their mutual benefit.

IDEA

The 67 counties in Pennsylvania represent the diverse nature of the commonwealth. They range from rural areas with small populations to large urban areas such as Pittsburgh and Philadelphia. Likewise, the resources available to these counties – human, financial, expertise, etc. – vary greatly. As a result, we see a great disparity in cybersecurity capabilities across counties with cases of *haves* and *have-nots*.



It is common for each county to stand up its own security services and solutions. Such an approach can result in the exhaustion of already scarce human resources, as well as duplication of efforts and increased cost and complexity. When multiplied across the various state and local government entities, these inefficiencies provide an opportunity to improve. Furthermore, citizens generally do not view the different levels of government as separate entities. State governments must do better in relation to ensuring that cybersecurity capabilities are more consistent across all levels of government and taking advantage of opportunities to partner so that we can provide the best value to taxpayers.

Each day, government networks are targeted by hackers working to compromise end users and network resources. Over the past twelve months, OA blocked 393 billion intrusion attempts against the commonwealth's firewalls (representing a 55% increase over the year prior). Despite best efforts to block such attacks, incidents will happen – it is not a matter of if, but when.

The human factor is always a significant security risk. End users open phishing emails and provide account credentials. They click on links and install malware on their computers. They download and open attachments with malicious payloads. Technical controls can help to mitigate this risk but can never fully eliminate it. In a recent three-month period, OA blocked over 96 million spam and malicious email messages. This represents 52% of all incoming email! Given such volumes and continually changing tactics by bad actors, some malicious emails will sneak through. Therefore, organizations must rely on their end users to exercise due care to avoid a security incident.

Proper and effective monitoring must be in place to protect network assets and enable a rapid response to an incoming attack. Without the ability to see what is happening in as close to real time as possible, an organization cannot take the necessary steps to swiftly contain an attack, giving the attacker the opportunity to fully exploit their entry, potentially exfiltrate data and spread laterally to other connected systems. A single incident could result in an attacker obtaining access to the networks or systems and any data they may contain. It is critical that all 67 counties in Pennsylvania have proper network monitoring in place. It is also critical that such a service be managed centrally to enable a holistic view of the interconnected entities and to provide an enhanced, correlated perspective into events that may be happening statewide.

IMPLEMENTATION

In 2016, OA and CCAP partnered to collaborate and foster relationships between local governments and the state. This effort provided an avenue to identify and pursue opportunities to collectively improve as one. Joint quarterly meetings called CyberSafe were established for county CIOs and state cybersecurity officials to discuss the myriad of challenges that we all face, opportunities to partner and how we can leverage each other's skills to further improve the security posture across different levels of government. Eventually, as the quarterly work group meetings matured, it spurred the introduction of additional work groups that also met regularly to share information and identify opportunities to improve election security and end user security.

It is through these collaborative work group meetings that new ideas were born to collectively improve cybersecurity across the state, formulate new ideas and ask bold questions such as:

- What if we could work together to deploy shared services for end user cyber security awareness training and phishing testing across all users in state and county government?
- What if we could leverage existing tool sets used by OA and make them available to our county partners so that they can enable capabilities they did not previously have due to costs, limited resources and other general challenges?
- What if we could achieve economies of scale, reduce overall costs, maximize efficiencies, improve knowledge transfer, reduce duplication of work and reduce the haves and have nots, which continues to be one of the most significant challenges faced by state and local governments?

In response, the state and county teams collaborated to further their partnership by establishing a shared service model to meet state and county objectives.

In 2019, the OA and CCAP collaborated on a shared service which would meet all state and county objectives. Collectively, the groups collaborated on a business plan to provide security awareness training and phishing exercises for up to 150,000 county and state users through a single shared service.

The state and county teams identified through governance processes what was needed in such a shared service. The group collectively created and submitted a detailed business case and proposal with five separate options, which was presented to the IT governance committee. The business case included benefits and drawbacks for each option, alternatives and analysis, costs for each option with quotes and the return on security investment (ROSI) to quantify the monetary value back to the business.

By identifying the return on security investment in the business case, the team was able to articulate how putting together such a service makes sense, not just from an economic perspective, but also how it would safeguard state and county systems and users from cybersecurity threats, increase user productivity and provide real benefits to the business and taxpayers. Through this process, the team was able to garner approval to proceed with the project and jointly decided on the shared service tooling that would be leveraged to meet collective business needs.

While counties can leverage state procurement contracts for their own purchases, they are unable to achieve the bulk licensing discount rates that the commonwealth enjoys. By combining the counties' license needs with those of the commonwealth into a single procurement of 150K licenses, OA was able to provide a service that benefitted all and achieved an economy of scale beyond that of the commonwealth alone. This gave all counties access to the training and phishing exercise capabilities, which they both wanted and needed. In addition to the licenses for the third-party service, OA made the commonwealth's cybersecurity training materials available for use by the counties.

Today, each county has its own tenant in the service that is not shared with the other counties or with the commonwealth. Each county conducts its own training and testing program.
This path has enabled OA to provide course completion and phishing click rate metrics to identify human risk on a county-by-county basis. For the counties that want to control their own training or exercises, they have that ability.

The positive outcomes of this initiative include:

- Enhanced security posture though an educated county workforce
- Reduction of overall costs through economies of scale
- Maximized efficiencies and reduced duplication of work
- Increased knowledge sharing
- Created streamlined and uniform processes and services.

CCAP and the counties have reported favorably on the program and OA will renew it for the upcoming fiscal year.

To build on the success of the shared services training program, OA sought to further strengthen the network perimeter security of Pennsylvania counties. Every county network connects at some level with state agencies in the commonwealth for data-sharing and other services. A successful attack on any county network has the potential to spread laterally through the county. Such an attack could impact services with the commonwealth and even possibly within the commonwealth network.

As one can imagine, there is no unified or even a standardized network architecture among the 67 independent counties. Collaborating with CCAP and the counties to bolster such a patchwork of networks was not feasible with the available resources at the commonwealth. Instead, OA sought to enhance the detection and response capabilities of the collective community.

This program started with OA sponsoring all counties with memberships in the Multi-State Information Sharing and Analysis Center (MS-ISAC) and in the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC). MS-ISAC and EI-ISAC are operated by the Center for Internet Security (CIS) and provide their members with many resources to support cyber defense, often at no cost. These resources include sector-specific threat intelligence products, incident response and remediation, threat and vulnerability monitoring, cybersecurity awareness and training products and tools for implementing security best practices. This enhances the counties' capabilities for incident response as well as awareness of the threat landscape.

As a second part of the network enhancement program, OA and the PA Department of State (DOS) collaborated with MS-ISAC and CCAP to deploy Albert Sensors to each county. The Albert program is an Intrusion Detection System (IDS) run by MS-ISAC and is installed at each county as part of its network perimeter. The MS-ISAC Security Operations Center (SOC) provides 24x7 monitoring of the Albert sensors and alerts the appropriate parties, including OA, of any potential malicious activity or attack. Already, sensors have been deployed to 2/3 of the 67 counties. These services enhance the counties' detection and awareness of any potential malicious activity or attacks against their networks and enables them to respond more rapidly, before the perpetrator can do more extensive damage. It also provides OA with awareness and insight across the extended county and commonwealth network perimeter.

IMPACT

The outcomes of these cross-collaborative efforts have helped to achieve more consistent cybersecurity capabilities across all 67 counties in Pennsylvania and to improve the common security posture across local government.

Utilization by counties of the security awareness and phishing exercise shared service in 2020 includes:

- 61 counties conducted or participated in at least one phishing exercise
- 20 counties conducted and/or participated in 4 or more phishing exercises
- 5 counties conducted and/or participated in 9 or more phishing exercises
- A least 14 counties leveraging the LMS functionality, which can be used to deliver training on any topic in addition to security awareness training

From a business value perspective, the return on security investment (ROSI) in implementing the security awareness and phishing training shared service has resulted in real dollars saved. For example, it costs organizations a minimum of $234 per user to wipe an infected PC and reset a compromised account. Assuming only 4% of the users fell victim to phishing emails and compromised their accounts, the IT costs run about $1,534,000. This does not include lost productivity or the potential cost of a breach. With the annual cost of the shared service at $190,000, we see an ROSI of about $1,344,000, making it well worth the annual investment to train end users and reduce the overall hard costs associated with end user risk and phishing attacks.

The initiative has:

- Strengthened the state cybersecurity posture and election security via partnerships and cross-collaboration with CCAP
- Established a unified shared service providing security awareness training and phishing exercises for all 150,000 employees/contractors across state and county governments

- Created and optimized the shared services model and bolstered overall security
- Reduced overall costs, achieved economies of scale, maximized efficiencies, reduced duplication of work, improved knowledge sharing and stronger collaboration and coordination across state and local government
- Spawned new opportunities to expand the services beyond counties to local school districts and city governments across Pennsylvania
- Enabled all 67 counties to conduct phishing exercises AND conduct security awareness training (or any other type of training) via a common unified shared service.
- Improved election security and assisted the Department of State with its business objectives related to securing elections.
- Aligned with strategic concepts associated with cross-collaboration and partnerships.
- Achieved economies of scale to lower overall license costs by up to 50% and established a common training platform and service for all state and county users.
- Reduced duplication of architecture, tooling and work and created an even playing field for all.
- Bolstered cybersecurity capabilities across state and local government.
- Made MS-ISAC Albert sensor network monitoring services available to all counties.

Due to the overwhelming success of this standardized cross collaboration partnership model and shared services approach, OA is in the process of expanding its partnerships with the counties by adding additional services such as enhanced information and intelligence sharing. In addition, OA is also expanding cross-collaboration and shared services to other areas of local and state government including the four caucuses of the General Assembly, school districts, cities and higher education.

We believe that building new relationships, fostering existing relationships, working horizontally across jurisdictions, building collaborative influence and earning trust is a repeatable recipe for success. Such an approach can be applied by other states or other areas of government where synergies for success can be identified, realized and optimized for the greater good of cybersecurity for all and value for taxpayers.