pennsylvania
OFFICE OF ADMINISTRATION

Enhancing Local Government Cybersecurity Through Collaboration and Shared Services

A Repeatable Approach for Success

Category:
Cybersecurity

Nominator:
John MacMillan,
Chief Information Officer

Commonwealth of Pennsylvania
1 Technology Park
Harrisburg, PA 17110
CIO@pa.gov

Initiation: July 2020

Completion: March 2022

EXECUTIVE SUMMARY:

Pennsylvania has more local governments than any other states except Texas and Illinois. According to the 2017 Census of Governments, there are nearly 5,000 active local governments, which include counties, municipalities and school districts.

As in many other states, our 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. This interconnectedness means that a lack of cybersecurity resources and capabilities in one organization can create additional risk to others.

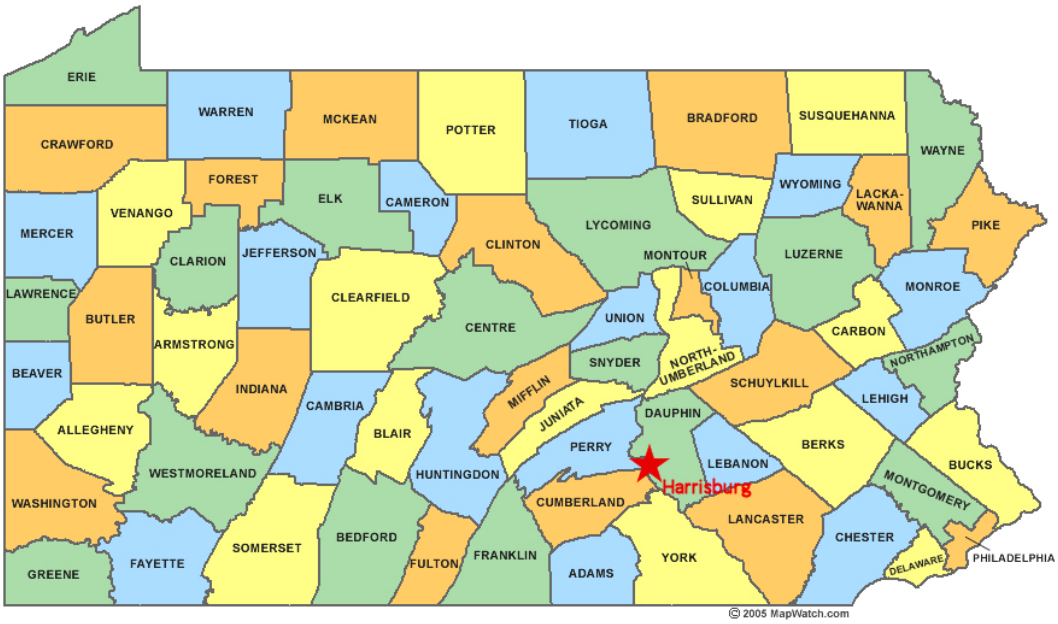
To strengthen overall election security in Pennsylvania and to further the Enterprise Information Security Office's mission to mature the commonwealth's overall cybersecurity posture, the Office of Administration (OA) is partnering with local governments to provide cybersecurity programs and other shared services. Through our partnerships with the County Commissioners Association of Pennsylvania (CCAP) and the City of Philadelphia, OA has provided copies of its own security awareness training materials, including an interactive web-based course. Additionally, OA leveraged the commonwealth's buying power to achieve economies of scale in the purchase of licenses for a third-party security training and testing service. Today, each participating local government has its own tenant in the service that is not shared with the other participants or with the commonwealth. This initiative is bolstering security, aligning with best practices, achieving economies of scale, reducing of overall costs, maximizing efficiencies, increasing knowledge transfer, reducing duplication of work and streamlining processes and services. The cost to implement end user security awareness training and exercise capabilities as a shared service was 50% less compared to the cost if OA and participating local governments had procured them individually. The local governments that are currently participating have reported favorably on the program and it will be renewed for the upcoming fiscal year.

OA undertook another program 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 46 of the 67 counties.

OA is in the process of expanding its partnerships with the counties by adding additional services such as enhanced information and intelligence sharing. 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 institutions for higher education. OA believes that building new relationships, fostering existing relationships, working horizontally across jurisdictions, building collaborative influence and earning trust is a repeatable approach that can be applied by other states and areas of government to enhance cybersecurity for all and value for our taxpayers.

IDEA

The Commonwealth of Pennsylvania is comprised of 67 counties, over 2,500 municipalities, 500 school districts and various other political subdivisions. The resources available to local governments – human, financial, expertise, etc. – vary greatly. As a result, there is a great disparity in cybersecurity capabilities with cases of *haves* and *have-nots*.



Each day, government networks are targeted by hackers working to compromise end users and network resources. If users fall victim or networks are compromised, passwords and other data can be obtained or exfiltrated and business systems can be negatively impacted. Despite best efforts to block such attacks at the state and county levels, incidents can and do 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 that install malware on their computers. They download and open attachments with malicious payloads. Technical controls can help to mitigate this risk, but it can never be eliminated. In a recent three-month period, the Office of Administration (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 evade efforts to block them. Therefore, organizations must continue to rely on their end users to exercise due care to avoid a security incident.

To protect network assets, proper and effective monitoring must be in place to 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. 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 state-wide.

IMPLEMENTATION

In 2016, the Office of Administration partnered with the County Commissioners Association of Pennsylvania (CCAP) to collaborate on cybersecurity and to build and foster relationships across government. Quarterly meetings called CyberSafe were established to provide an avenue for county CIOs and state cybersecurity officials to discuss the myriad of challenges that we all face and identify opportunities to partner. The CyberSafe meetings spurred the creation of additional election security workgroups to share information and have more focused discussions regarding election and end-user security. These collaborations sought to collectively improve cybersecurity across the state and reimagine how state and local governments can work together more effectively. For example:

- What if we could work together to provide the ability to conduct cyber security awareness training and phishing exercises across all users of state and county government?
- What if we could leverage existing tool sets used in the state and make them available to our county partners so that they could 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 remove the *haves* and *have-nots* which has historically been one of the most significant challenges facing local governments.

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

From 2019 to 2020, OA worked with the counties to identify the requirements for a shared service to address end user security awareness training and exercises. 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) which would identify the monetary value back to the business.

By identifying the ROSI in the business case, the team was able to articulate how creating the service made sense, both from an economic perspective as well as safeguarding state and county systems and users from cybersecurity threats, ultimately showing real value to the taxpayer. Through this process, the team was able to garner approval and funding to proceed with the project and jointly decided on the details surrounding the shared service.

The commonwealth itself has had an effective, interactive training program on general security awareness, including the proper handling of email – danger signs of a phishing

email, hover technique for links, reporting of potential malicious emails and so on. This training is updated annually, and all employees and contractors are required to complete it annually. The training is tested with regular phishing exercises conducted through an external vendor several times a year. The vendor is able to host cybersecurity training (and provides such course material), though the commonwealth itself does not utilize this feature in lieu of using its own enterprise training service.

While local governments can leverage state procurement contracts for their own purchases, they are unable to achieve the bulk licensing discount rates that the commonwealth enjoys. Based on the collaborative teamwork, OA combined the counties' cybersecurity training needs with that of the state government into a single procurement of 150,000 user licenses for the third-party training service. OA was able to provide a service that benefitted all and achieved an economy of scale beyond even 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 local governments.

Today, each county and the City of Philadelphia has its own tenant in the service that is not shared with the other participants or the commonwealth. This approach enables OA to provide course completion and phishing click rate metrics to identify human risk on a county-by-county basis, while giving each organization the autonomy to conduct its own training and testing program. The positive outcomes of this initiative include:

- Enhanced election security though an educated local workforce
- Reduction of overall costs through economies of scale
- Maximized efficiencies and reduced duplication of work
- Increased knowledge sharing
- Streamlined and uniform processes and services.

CCAP, the counties and the City of Philadelphia 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 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.

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. 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), which provides 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. Membership enhances the counties' capabilities for incident response and heightens 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 46 of the 67 counties. These services enhance the counties' detection and awareness of any potential malicious activity or attacks against their networks and enable them to respond more rapidly. It also provides OA with awareness and insight across the extended county and commonwealth network perimeter.

IMPACT

During 2020-21 fiscal year, the counties took the following advantage of the training/testing program:

- 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

From a business value perspective, the return on security investment (ROSI) in implementing security awareness and phishing training as a shared service has resulted in actual dollars saved. For instance, it costs a minimum of $234 to wipe an infected PC and reset a phished user account. Assuming only a 4% rate of state and local government users compromising their devices and accounts through phishing, remediation of these incidents would cost approximately $1.40 million per year. This doesn't include lost productivity or the potential cost of a data breach. With the annual cost of the shared service running $190,000, we estimate ROSI of about $1.21 million.

The initiative has:

- Strengthened the state cyber security posture and election security via partnerships and cross collaboration with local government entities
- Established a unified shared service providing security awareness training and phishing exercises for all 150,000 users across state and local government
- Created an optimized shared services model, and bolstered overall security
- Has reduced overall costs, achieved economies of scale, maximized efficiencies, reduced duplication of work, improved knowledge sharing and has resulted in better 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 PA
- Improved election security and assists Department of State with its business objectives related to securing elections
- Aligned with strategic concepts associated with cross-collaboration and partnerships
- 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

OA is building on the success of this standardized cross collaboration model and shared services approach by partnering on additional services such as enhanced information and intelligence sharing. 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 institutions for higher education. The Office of Administration believes 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 our taxpayers.