Hearing on Cyber Security for Cybersecurity Issues for Local Governments and Municipal Authorities

Testimony by John Alwine
Unisys Public Sector, Region Director – Commonwealth of Pennsylvania

Cliff Shier
Unisys Managing Principal, Cloud, Infrastructure, and Applications
and
Tom Guenther
Unisys, Business Relationship Manager- Commonwealth of Pennsylvania

Before the Senate Communications and Technology and Local Government Hearing

Wednesday, January 31, 2024

The Honorable Tracy Pennycuick, Republican Chair and Honorable Jimmy Dillon, Democratic Chair.

Thank you for the invitation to testify before you on behalf of Unisys regarding cybersecurity. It is Unisys' position that while many large businesses and various industries have been focused on their own security and defensive measures over the past decade, to varying degrees of success, the public sector has had numerous obstacles to prepare for and respond to the significant threat to their critical systems and information. Whether it be protecting personally identifiable information such as tax records, unemployment claims or social security numbers, or the systems that allow them to administer licenses, distribute unemployment checks or collect tax receipts, for too long government has been restricted by funding and staffing constraints hampering the ability to move off outdated systems and to secure their most important assets. Unisys believes that taking critical steps towards supporting and enhancing the Commonwealth's security environment will mitigate risk to continued operation and bolster public trust and the reputation of all Commonwealth's government entities.

Our testimony will provide a measured approach, recognizing that the Commonwealth does not have unlimited financial resources to put towards cybersecurity, nor does it have the extensive staffing support necessary to carry out all recommendations internally. Within the time constraints of this hearing, it will not be possible to go beyond our initial set of recommendations, but we will highlight four actions that we believe will support ongoing State and County government's activity while also putting Pennsylvania farther down the road to a stronger security posture.

`

About Unisys

My name is John Alwine and I serve as Unisys' Region Director for Pennsylvania as well as being a life-long resident of the Commonwealth, having grown up in Dauphin County and graduating from Shippensburg University. Unisys is a global technology leader with headquarters in Blue Bell, Pennsylvania, that builds high-performance, security-centric solutions for the most demanding businesses and governments. We provide services to over two dozen states with offerings that include security solutions, advanced data analytics, cloud and infrastructure services, application services, and application and server software. We have a strong focus on digital government and specialized expertise in leading practices across public sector entities, including security operations. More importantly, we are a company rooted in Philadelphia, Pennsylvania. It is where we developed the world's first commercially available computer system in collaboration with the University of Pennsylvania in 1945. Unisys is proud to be a trusted advisor and supplier of IT services to Pennsylvania, the Commonwealth's largest information technology partner. For decades, Unisys has successfully collaborated with the Commonwealth to provide reliable, cost-effective and mission critical services to Pennsylvania government agencies and citizens. Unisys' digital services have streamlined state operations, saved taxpayers millions of dollars, ensured public safety, and improved the ability of Pennsylvania citizens to obtain online access to valuable information and government services.

In June 2014, Unisys and the Commonwealth launched a first-of-its-kind initiative that transformed how state agencies could acquire IT services. Through this initiative, called Pennsylvania Compute Services, or PACS, Unisys invested $77M and is providing and operating one of the largest, Criminal Justice Information Security (CJIS) protocol secure, private cloud-based, on-demand IT computing implementations by a state government for a few of the commonwealth agencies. Under the competitively awarded PACS contract, Unisys consolidated some agency data centers into a secure private hybrid cloud that enables agencies to access IT services as needed within the Unisys owned-managed PACS data center, protecting the citizens' data while enhancing flexibility and service delivery.

It is safe to say our experience in the Commonwealth and across the country has enabled us to understand best practices for states' IT operations, including their security posture. These best practices help drive better understanding of IT security needs, the need for greater coordination and cooperation amongst state entities and between the public and private sector, and efforts that protect critical systems and data in a cost-effective and efficient manner.

We believe that the Commonwealth can take specific actions to enhance their security posture at a time when the public sector faces more extensive cybersecurity risks than ever before.

`

Cyber Risk in Government

In a recent 2023 study by Sophos, it was revealed that the rate of ransomware attacks in the state and local government organizations continues to rise: 69% of state and local governments reported that they were hit by ransomware, up from 58% in 2022. The common theme for organizations is "not if, but when."

The report indicates the rate of ransomware attacks in state and local government organizations in the 2023 study was above the cross-sector average. Across all sectors, education was most likely to be hit, with 80% in lower education and 79% in higher education reporting an attack. IT, technology, and telecoms reported the lowest attack level (50%), indicating increased cyber readiness and defenses.

Within state al local sectors 69% of them were compromised by ransomware and 34% of those ransomware victims paid ransom. Last year, the average cost to remediate a ransomware attack in the government sector rose to $1.07 million, more than five times the previous year's average of $231,000. The average payment also increased with 25% paid over $1 million, as the payments under $100,000 shrank. Once the data is recovered the average cost to remediate the attack is $1.2M with private sector paying on average $1.8M.

Key Elements for a More Secure Cybersecurity Structure

Quickly transitioning from a state of vulnerability to a locked down environment where cyber-attacks are addressed in a timely manner and damage is minimalized (because attacks will never be 100% prevented), is not something that can be accomplished overnight.

Unisys understands that cybersecurity and information technology has become more complex since the start of the pandemic, let alone over the past decade. State governments have struggled to react, often because of difficulty in adopting to emerging technologies, overcoming procurement requirements designed for defined items such as keyboards or printers and hiring and retaining internal personnel with the skillset to best leverage new tools and expectations. None of these issues is unique to Pennsylvania; these are challenges Unisys has witnessed across the country. States are adopting to the idea that security must be addressed in a holistic, whole-of-government approach.

While IT has often approached cybersecurity gaps as technical conversations about the newest firewall, adopting the latest virtual private network trend or signing up for security tools without having the ability to successfully manage their adoption; today, it is instead a strategic risk-based conversation about meeting increasingly complex agency needs while securing significant amounts of data and ensuring its recovery capability.

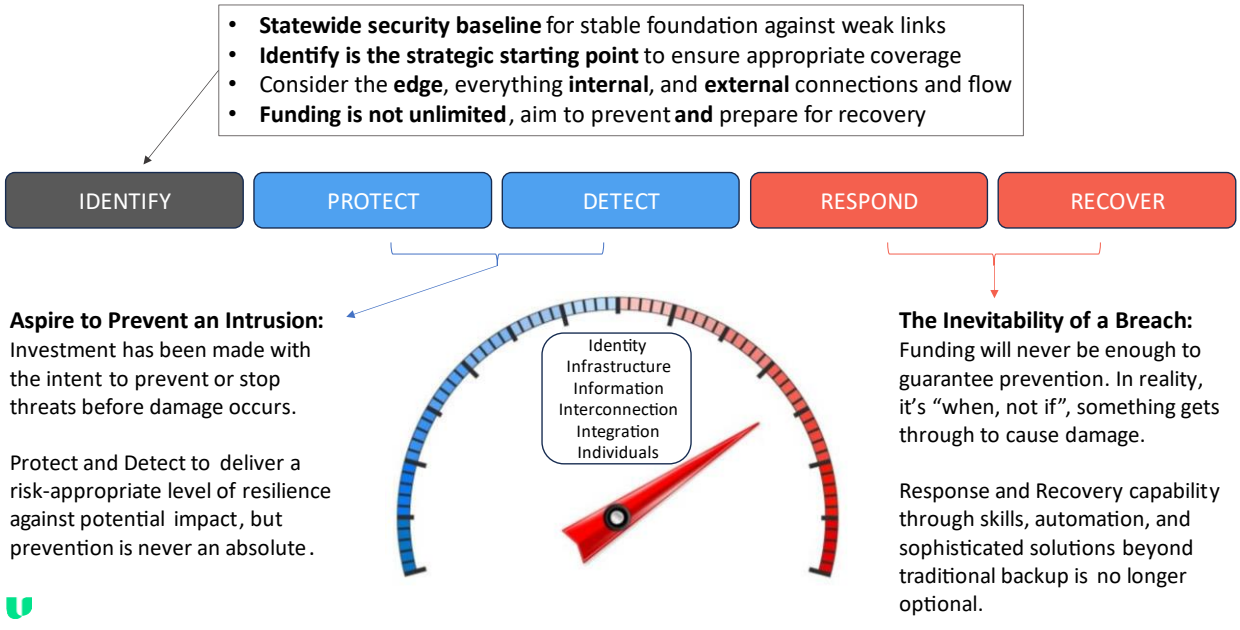
`

Noting that funding is not unlimited, and thus never enough to be able to provide absolute assurance of protection, cybersecurity strategies need to consider both the “ounce of prevention” and the “pound of cure”.

As such, Unisys recommends four key actions to help the Commonwealth define its risk profile, understand how to most efficiently utilize available funding to maximize return and make significant strides towards a stronger, more resilient cybersecurity framework. The four actions listed here are all important, and when performed together they are a robust path toward resilience:

- Adopt a Statewide security baseline, enforced as formal policy, requiring a specific minimum level of hygiene and rigor across all Commonwealth Agencies, to eliminate weak links, whether technology is individually deployed or as interconnected systems, and whether data is held in a datacenter, in the cloud, or in the hands of a third-party.
- Since the protection boundary, or “edge”, continues to expand and become much less well-defined, continual evaluation, monitoring, and governance are essential for clarity on all aspects regarding the risk-appropriate extension of protection measures and mechanisms.
- Aspiration to prevent an intrusion has been where the majority of investment has occurred, and that should continue to be the primary focus of optimization and rigor. Being intent on doing everything possible to stop attackers before they inflict damage is unfortunately a never-ending process. For simplicity in making this point, there are six “I”s to focus on as vectors of attack (Identity, Infrastructure, Information, Interconnections, Integrations, and actions by Individuals).
- The focus on recovery is more important than ever. The number and sophistication of attacks, and their success at achieving their various goals, delivers a clear message that it’s not if, but when, a breach will occur. Such an inevitability mandates the capability to respond and recover from a security incident. Due to the sophistication of advanced persistent threats, conventional backup strategies commonly used in the industry lack the functional capability to ensure recovery from the most serious and damaging incidents.

The Strategically Resilient Digital Environment



Conclusion

Unisys appreciates this Committee's efforts to learn more about the cyber risks of all governmental agencies irrespective of their size or financial capacity. The federal funding from the Infrastructure Investment and Jobs Act provides an opportunity to improve cybersecurity and risk management efforts. The legislature, current Administration and Local government leaders must continue efforts to develop, implement and enhance a strong cyber resiliency program to that can identify, protect, detect, respond, and recover from cyber-attacks.

The technology workforce challenges facing public sector agencies require interaction and cooperation with private sector entities to provide resources and leading-edge tools to protect critical infrastructure and sensitive data. Working together, the private sector can provide insight and feedback on the Commonwealth's strategic and tactical vision as well as providing highly skilled resources that can protect against the ever changing and expanding threat environment.

To achieve short and long-term resilience and security we recommend leveraging the current federal cybersecurity funding, establishing strong strategic governance practices, increasing investment in cybersecurity efforts, and creating a reliable recovery platform for when an incident happens that can provide for rapid response.

We recognize that each of the four key actions we outlined could be entire conversations on their own, and to these ends, Unisys is pleased to offer our thoughts, and appreciates the recommendations made by others testifying before your committee. We look forward to continuing to work with the legislature and the Administration to address these important security issues and to find new ways to allow the state to take advantage of security innovations that produce better results in a more secure manner for agencies and residents. Thank you for the opportunity to testify and to share our views, and I welcome any questions you may have.

`