4250 Crums Mill Rd, Suite 105
Harrisburg, PA 17112
www.unisys.com

Hearing on Cyber Security for Cloud-based Government Applications

Testimony by:
John Alwine
Unisys Public Sector, Region Director – Commonwealth of Pennsylvania
and Cliff Shier
Unisys Managing Principal, Cloud, Infrastructure, and Applications

Before the Communications & Technology Committee
Senate of Pennsylvania

March 13, 2023

The Honorable Tracy Pennycuick, Chair

Chairman Pennycuick and members of the Committee, thank you for the invitation to testify before you on behalf of Unisys regarding cybersecurity for Cloud-based Government Applications. 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 been too slow to realize the significant threat to their own critical systems and information. The threat to the critical data is real and needs to be addressed whether the systems are on premises or in the cloud. Whether it be protecting personally identifiable information such as tax records, unemployment claims or social security numbers, or the systems that allow the Commonwealth to administer licenses, distribute unemployment checks or collect tax receipts, for too long government has utilized outdated approaches to secure their most important assets.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 the 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 Strategy, Governance, and Zero Trust as three actions that we believe will support ongoing Commonwealth activity while also advancing Pennsylvania farther ahead on the road to a stronger security posture.

Our testimony will focus on helping identify the right actions for delivering results for the Commonwealth as it relates to protecting critical data and systems via the use of information

technology (IT) in state government. Our comments reflect best practices across other states and the federal government and leverage our own experiences as well as extensive expertise by individuals within Unisys.

It is our intent to share critical information that both informs this committee and provides a potential roadmap that, when done in coordination with the Commonwealth's IT leaders, produces a safer and more secure operational environment.

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. I am joined here today by Cliff Shier, Managing Principal within our Security Services group. 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 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. Under the competitively-awarded PACS contract, Unisys consolidated data centers into a secure private hybrid cloud that enables agencies to access IT services as needed, protecting the citizens' data while enhancing flexibility and service delivery available to more than 45 state agencies, boards and commissions.

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.

Current World Affairs Are Accelerating The Security Risk to Critical Entities

Verizon's 2022 Data Breach Investigations Report reported that public sector organizations were involved in one-in-five cyber incidents, amounting to roughly 2792 cyberattacks. Their data also revealed that approximately 47% of public sector data breaches were not discovered until years after the initial attack. This delayed discovery allows criminals more time to steal information and wreak havoc while avoiding detection and responsibility for their crimes.

International conflicts aside, the pandemic has had, and will continue to have, an impact on security needs as the Commonwealth and other states accelerate their digital transformation efforts to meet a new operating involvement. No longer are all employees expected to be in one state-owned location all the time. The work from home / hybrid work approach brings with its new demands, as do initiatives to move data and operations to a cloud environment.

The risk to any individual or organization, private or public sector, has never been greater. No longer are private sector entities the sole target for cyberattacks; state and federal government agencies, departments and educational institutions are making up a growing proportion of all attacks. The reputational and economic exposure has grown exponentially in response to world affairs, and many individuals and organizations – including the Commonwealth - are inadequately prepared for the consequences of the severity of the possible negative outcomes. News reports of breaches have become a near daily occurrence. Most of us have been issued new bank cards at one time or another well in advance of the expiration dates as a response to some of these breaches. Worse yet, when protected or private personal data is shared because it can be, not because it should be, the opportunity for misuse escalates, along with the risk of reputational damage and of course the potential for litigation. It is critical that public and private sector entities take a collaborative approach to security, leveraging each other's strengths and abilities to increase the security of critical systems and data.

Cyber Security for Cloud-based Government Applications

Cybersecurity components protecting cloud environments have a distinct advantage over many traditional or legacy datacenters in that the technologies and methods used are comprehensive and modern. The incorporation of these components does enhance defensive capability but does not automatically, continually, nor entirely secure all aspects of your workloads and data.

It is our position that major cloud platforms do inherently by design provide excellent security capabilities when leveraged appropriately. Cloud vendors encourage full usage of those capabilities. It is also our position that as new technologies and platforms emerge new attack vectors also emerge, requiring a rethinking of security in, to, and from the cloud – the networks, applications, devices, access, identities, data protection and stewardship, and more.

Securing cloud environments is a shared responsibility between the organization and cloud vendors. Managing that demarcation is more complex than simply defining it. Further complication is introduced due to interoperability challenges between differing mechanisms that protect legacy and cloud architectures.

When presenting to audiences regarding the need for a comprehensive cybersecurity strategy invariably someone will ask a question about technology products to deploy. Unfortunately, the path to good security is not as simple as selecting toolsets or hardening an extended perimeter.

Vulnerabilities and threats are two sides of the security equation. Considering employees, contractors, suppliers, and other 3rd parties involved, these are not strictly internal or external concerns. New vulnerabilities are discovered daily. Organizations commonly assess for those known vulnerabilities and deploy patches as a countermeasure. Modern cloud architecture supports expedient patching, but legacy systems shifted to the cloud without transformation often hinder that process. Threats are also in need of continual assessment because attackers are actively targeting victims, operate with agility, incorporate advanced automation, and are continually evolving their methods. Exploits are unleashed against known and unknown vulnerabilities, and well-funded attackers are motivated to utilize the most modern and advanced weapons against your defenses.

While roughly 18% of Public Sector attacks are aimed at espionage or disruption, 80% are financially motivated. Attackers are focused on how to extract the optimal financial reward offered by selling your data, whether back to you, or to someone else, or both. They are not concerned about your recovery if you're not intending to pay the ransom. For these reasons, the strategic refocusing of investment in both legacy and cloud security (Networks, Identities, Data, and People) would enhance the resilient and secure delivery of crucial services.

Zero Trust is a concept that has recently become more mainstream but has existed for over a dozen years. There are toolsets that in principle enable and support the concept, but security will never be a "one size fits all" solution or a "set it and forget it" discipline.

One of the key tenets of Zero Trust is "assumed breach". Frameworks, standards, and best practices assist in defining and assessing a well-planned defense-in-depth posture against attacks, but the reality is that no amount of rigor or spending can entirely prevent a breach.

This is especially true in the Public Sector, where negatively impactful outcomes have been increasingly experienced all around the nation. We recognize that investment is not unlimited, but there is much

that can and must be accomplished within the Commonwealth in a prudent and risk prioritized manner. Beyond managing technical and operational controls, effectiveness is optimized when proactively bounded by a well-aligned risk-focused strategy and overarching governance.

Cybersecurity is no longer a challenge to be met from whatever remains of an agencies' information technology budget. As recently as 2020, fewer than 40% of states had a dedicated budget line item for cybersecurity, and half of states were allocating less than 3% of their total IT budget to cybersecurity. That approach has begun changing, driven as mentioned, by global events, but in no way has state spending reached what most cybersecurity experts would say is a satisfactory level. According to the 2022 Public Sector Cybersecurity Survey Report by SolarWinds, 50% of state government respondents and 25% of local governments indicated that budget constraints are an obstacle to maintaining or improving IT security.

The federal government has either given states and localities flexibility to spend federal recovery dollars on cybersecurity initiatives (CARES Act) or directly appropriated funds for use to meet rising cyber challenges (ARPA). In the Infrastructure and Investment Jobs Act, passed late last year, the federal government designated over $2 billion in funding for cybersecurity resiliency and innovation. The bill includes funds to reduce cyber vulnerabilities in public water systems and drinking/clean water technology. Additionally, the bill allocates state and local funding via grant programs for cyber functions to include detecting and recovering from cyber threats and emergencies. The law requires states to create cybersecurity plans in order to receive grants.

At the state level, legislators are including specific line items to support cybersecurity efforts. Some recent examples of states appropriation dollars specifically for cybersecurity initiatives:

- Florida will provide $87+M to fortify cybersecurity in the state, including $50M to "Enterprise Cybersecurity Resiliency".
- The Virginia House of Delegates submitted its version of the state's budget, allocating $150 million for cybersecurity initiatives for the next two years
- Texas created a Technology Improvement and Modernization Fund to improve state agency information resources, with $898.6M to support state cybersecurity and legacy system projects. Maine appropriated state and federal recovery funds to tackle the highest-cyber risk areas identified by an external program review, including formalizing a business continuity plan for the State's information technology, as well as other identified cybersecurity programs.

Additionally, states such as Minnesota, Montana and Washington included specific cybersecurity initiatives in their budgets as a means to focus their own state's IT agencies on cybersecurity initiatives rather than leaving all funding in one large IT pot.

It is imperative that states, including the Commonwealth, provide necessary funds to support improvements in their security posture or their reputational, operational and legal implications will continue to increase.

Conclusion

Unisys applauds this Committee's efforts to learn more about the cyber risks facing cloud-based government applications. While it is important that all levels of government work with the private sector to provide resources and tools to protect critical infrastructure and sensitive data, it is equally urgent that government turn the risk mirror upon itself to understand its own vulnerabilities as well as consideration of internal and external threats. The legislature and Administration must seek out increased coordination amongst state IT users, foster greater recognition of security risks for state agencies, holds government IT leaders accountable in establishing a security path forward, but also provides the resources necessary to implement such a strategy.

Like most states, the Commonwealth faces a continuing challenge to maintain and improve the quality of services it provides, while dealing with an ever-changing technology environment. Other states are overcoming the lack of funding by leveraging the Federal (ARPA) funds and investing Millions of dollars to establish the Governance and systems to protect their citizens data.

To achieve long-term resilience and security we recommend to increase investment in such strategic cybersecurity efforts and the addition of overarching governance as well as continued advancement of protection and detection, minimization of impact, and the crucial expectation of the need to recover from a breach. Beyond managing technical and operational controls, effectiveness is optimized when proactively bounded by a well-aligned risk-focused strategy and overarching governance.

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.