UNISYS | Securing Your Tomorrow®

Hearing on data privacy and potential updates to the Breach of Personal Information Act

Testimony by
Clifford Shier, Managing Principal
Unisys Public Sector | Enterprise Solutions | Security Solutions
CGEIT, CCISO, CISM, CSMP, Six Sigma, ITIL, ISO Internal Audit

Before the
Senate Communications & Technology Committee
Pennsylvania Senate

February 5, 2020

The Honorable Kristin Phillips-Hill, Chairman

Chairman Phillips-Hill, Chairman Kearney and members of the Senate Communications & Technology Committee, thank you for the invitation to testify before you on behalf of Unisys regarding data privacy. It is Unisys' position that collaboration on data protection and privacy is both urgent and timely. Steps toward positive outcomes for data protection and privacy, and assurances communicated in this regard, will bolster public trust and the reputation of the Commonwealth's government entities.

My testimony will provide a measured perspective on the general topic of data protection and privacy, and will do so regarding key aspects of the inherent disciplines, risks, and responsibilities. Within the time constraints of this hearing, it will not be possible to cover disciplines such as Data Classification and Data Lifecycle Management at depth, but I will highlight some of the nuances that Data Privacy regulation brings to the forefront, and am open to participating in further dialogue on these matters.

About Unisys and Representation

My name is Cliff Shier and I am a resident of the Commonwealth, having lived in Monroe County for more than 17 years. I am here today representing Unisys' Enterprise Solutions consulting organization, and as an experienced Chief Information Officer (CIO) and Chief Information Security Officer (CISO) am a trusted advisor to our client CIOs, CTOs, CISOs and other Senior IT leaders. In my role, I provide thought leadership and strategy on topics such as the Governance of Enterprise IT, Risk, Compliance, Security, and Privacy. I have been called upon regularly by Harrisburg University of Science and Technology and their Government Technology Institute to lecture on topics such as these, including as presenter and panelist on their Data Privacy Day event last week. The Commonwealth is one of my clients. I have had the privilege to advise and provide guidance to the Commonwealth's Office of Administration, IT Delivery Centers, and other Agencies.

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, transformation and modernization, and specialized expertise in leading practices across state, federal and global public sector entities.

Importantly, we are a company rooted here in 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 as 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. Unisys invested $77M through this initiative, called Pennsylvania Compute Services, or PACS. We provide and operate one of the largest, Criminal Justice Information Security 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 world has enabled us to understand best practices for data protection and privacy. These best practices help drive better IT outcomes, with better understanding and decision-making, greater coordination, and cooperation amongst state entities and between the public and private sector, enabled by efforts that enhance the value IT can deliver while doing so in a manner that reduces risk.

Data Security and Privacy

As background to my comments, I'll provide some context in brief. Regulations refer to Personally Identifiable Information, Protected Health Information, or Personal Information in general, but central to the theme is the core consideration of who actually owns the rights to the data, and in that regard the regulations are trending toward favoring the Data Subject, in other words, affording rights to the person whose attributes are recorded, and responsibilities to the entity that is in possession of or tasked with processing the data. This is important to be aware of because it subsequently obligates organizations, and particularly IT within those organizations, to think differently about data, how it is protected and shared. In broad terms, this data would include items recorded with or without implicit

or explicit consent, which are capable of connecting the dots to directly or indirectly identify a person, that person's descriptors, status, or activities, regardless of who initiated the creation, acquisition, or capture of a record, transaction, or other tracking information.

There is an inseparable linkage between security and privacy. The data protection afforded by security sits squarely within what is known as the CIA Triad which is comprised of **C**onfidentiality, **I**ntegrity, and **A**vailability. Yet, many of the latest privacy regulations contain guidance and requirements that extend the need for systems functionality beyond data protection.

As children, we've all learned that sharing our toys is a good thing. We've also been scolded by our parents for sharing too much of our private family information with others. These are the two sides of sharing, and likely the earliest occasion we learned of the need for data privacy. We share when appropriate, with permission, honestly, in context, and so on.

Organizations, both private and public sector, are in possession of data that was gathered at some point, for a particular purpose, but continues to simply exist, lingering on in perpetuity, awaiting some potential future useful purpose. This holds significant risk to both the Organization and the Data Subject. This is where disciplined Data Classification and Data Lifecycle Management are necessary. It is difficult to protect data without identifying what it contains, classifying it accordingly, managing where it is, and ensuring adequate governance and stewardship of that data. The concept of a well-defined and fortified perimeter no longer exists. When business units directly contract and use "systems as a service" or other cloud solutions apart from IT awareness, governance, or management oversight, these occurrences of what is known as shadow IT multiply the data identification and classification conundrum. In order to protect data, especially when data has not been completely identified and classified, or when data is shared into systems managed by other parties, whether that party is internal or external, it is good practice to ensure that foundational safeguards are in place. The concept of Zero Trust has become mainstream. Just like it sounds, trust must be validated and earned continually. This speaks to necessary disciplines governing the entire lifecycle of the data that go beyond assumptions or delegation of protection. Technical controls to limit potential exposure, such as microsegmentation of the network and dynamic isolation of data according to use case, and of course encryption for data wherever it exists or is in transit are well advised.

Data Lifecycle Management is an enterprise policy-driven approach that seeks to define stages in the life of data. It is generally portrayed as a neatly defined cycle from the birth of the data through its ultimate transfer, archival, deletion, or destruction. Traditionally, this cycle has managed sets of data, like a file or database, but now also requires the ability to granularly identify, extract, and/or expire individual data items from within the data set. Recent and evolving privacy regulations have prescribed use cases to be adopted at multiple points throughout the lifecycle, and even ahead of the lifecycle, in preparation for the creation, acquisition, or capture of data. As an example, this would

include timely removal of data items that no longer align to the intended purpose, rather than the perpetual possession of data because it may someday be useful for other purposes.

Much of this privacy related systems functionality, or allocation of financial or personnel resources to service these processes, has not historically existed. As current and new legislation is knocking at the door or even ready to break down the door, modernization of systems and the retirement of legacy systems must be top-of-mind, and need sufficient resources allocated accordingly. While both security and privacy would be best designed into systems early, at the outset, legacy systems are not provided a free pass. Resources aside, it is a daunting effort to retroactively incorporate this functionality into many of the existing systems and processes.

That's the technical side, but let's apply this to risk. The risk to any individual or organization, private or public sector, has never been greater. The reputational and economic exposure has grown exponentially, and neither individuals nor organizations are adequately 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.

Unisys has for the past 13 years conducted a regional and global survey known as the Unisys Security Index. The 2019 Unisys Security Index is based on national surveys of representative samples of 13,598 adult residents aged 18-64 years of age. Regarding the individual, this year's results indicate that globally 69%, and in the United States 63%, of the respondents are either extremely or very concerned about Identity Theft. This number is increasing and this is the category that is ranked highest on the chart, significantly higher than even personal safety, which in comparison scored only 49% globally and 42% in the United States. While being somewhat desensitized by the breach after breach of their data, these threats are real and individuals are rightly concerned. Lives are impacted significantly more than a subscription to credit monitoring will solve. This fear is fueling the push to define who really owns the data and to regulate its' classification and ensure a carefully controlled lifecycle. I have included a copy of our survey that can provide further insight and information on how individual view security in today's operating environment

In response, organizations need to be aware of the true level of their own economic exposure, whether due to fines or the overall impact. Sufficient resources can only be made available to solve Data Privacy issues when this risk is credibly quantified. Effective methods to quantify this risk do exist, and establishing this discipline with any organization is highly encouraged. If Equifax had known that the cost of their 2017 breach would exceed $1.3 Billion, they would have likely insured themselves for more than just a tenth of that amount and established greater rigor and posture.

Conclusion

In conclusion, this serious level of concern toward Identity Theft can be interpreted as but a symptom of something deeper. The issues and concerns around Data Privacy come down to matters of trust regarding data and its use, misuse, or disclosure. Data Protection and Privacy regulations have come to exist because of this mistrust. In order to ensure that organizations are equipped to reach the high bar set by these regulations, there is a need to ensure commonality and consistency of expectation across the domains of authority, and a centralized point responsible for collecting and maintaining information on data sharing and breaches that will better inform policymakers on the true scope of the problem, and thus the risk exposure, that the Commonwealth faces. Collaboration is necessary across the Commonwealth and its constituents, across States and the Federal government, together with the private sector, otherwise organizations will be hard-pressed to accomplish the behaviors that the well-intended legislation had aimed to achieve.

Like most states, the Commonwealth faces a continuing challenge to maintain and protect the data entrusted to state agencies and bodies, data that is then used to provide critical services to residents. We are in an era of enhanced risk as public sector entities continue to fall under attack from both common criminals and nation states. Pennsylvania must continue to take important steps to provide an appropriate level of protection and privacy for data in the government's hands in order to garner and benefit from the public's trust. Supported by, and working cooperatively with, a private sector that can provide insight and feedback on the Commonwealth's efforts will help to ensure Pennsylvania is at the forefront within this space.

This great land, the United States of America, is entrenched with the diversity of its people, but one discipline that should unify, is that of Data Privacy. 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 issues and to find new ways to allow the state to better provide for the protection of personal data.

Thank you for the opportunity to testify and to share our views, and I welcome any questions that you may have.