Written Testimony of Joseph P. Harford, Ph.D., CSDS
Founder and President, Reclamere, Inc.
Pennsylvania House Majority Policy Committee

Chairman Causer and members of House Majority Policy Committee. Thank you so much for the opportunity to provide written testimony about cybersecurity and the threats posed by predatory attackers in Pennsylvania. Your work on enacting policies and legislation to protect your constituents is critical to Pennsylvanians and has a direct impact upon the people I interact with each day.

My name is Joe Harford. I have the privilege and honor to serve as the Founder and President of Reclamere. Along with my business partner and CEO, Angie Singer Keating we operate a twenty-one-year-old information technology asset management company in Blair County that specializes in supporting the cyber security resiliency of our clients. We support clients in healthcare, financial services, education, and government. Reclamere is proud of the work that we conduct both here in Pennsylvania, across the United States, and internationally. In addition to my responsibilities as a business owner, I am an adjunct faculty member at Juniata College, teaching entrepreneurship in the business program. I also serve as a Walker Township Supervisor in Huntingdon County, and I volunteer as a member of the Pennsylvania NFIB Leadership Council. I share this with you so that you can have a better understanding of my background and my perspective on cybersecurity.

It should come as no surprise that data breaches and the damage caused by them are on the rise. However, what may be of interest is that this is not the way that it must be in our state government, businesses, or schools. Nor do we have to believe that a strong information security posture must be burdensome or expensive.

I want to commend you for investing your time to examine this important area of cyber resiliency and protection. As more of Pennsylvania's students go online in schools leveraging the power of the internet to learn and create knowledge, your efforts to develop effective policies will be paramount to protecting them. As the amount of information that is created, stored, transacted, and managed continues to grow exponentially, your work on future legislation will be critical to protecting our citizenry. As the global "Internet of Things," IoT services market grows from an expected $163.70 billion in 2021 to $188.80 billion in 2022 at a compound annual growth rate (CAGR) of 15.3%., your work on this legislation will be a critical catalyst to empower connected innovation and wealth generation. As remote work, increased automation, and artificial intelligence fundamentally change how we manage employees, manufacture goods, and protect our supply chain, your work on this legislation will be vital to supporting next-generation innovation and our leadership in the world.

This is a necessary and extremely relevant topic in our hyper-connected world. The Privacy Rights Clearinghouse reports that there have been more than 900,000,000 records compromised in over 4,000 U.S. breaches since April 2005. Numerous high-profile data breaches have appeared in the news in the last year. FBI data shows that Pennsylvania led all other states in ransomware losses in 2020 — more than $5 million — spread among 116 victims. Does this mean that Pennsylvanians do not care about the safety of their data, not at all? It means that both the private sector and state government need to identify ways to collaborate more effectively to minimize the damage. The truth of the matter is that no organization will ever be entirely "secure," but with a robust security risk assessment, a comprehensive risk action plan, and a thorough remediation strategy we can start to win back some ground.

As long as there is a black market for the sale of personal and financial data, and data breaches are attainable, cyber-attacks will continue. At the same time, we live in a society that demands mobility and connectivity. More Pennsylvania children are getting online at a younger age, and more and more of our household devices are connected to the internet. This ever-present connectivity makes sound information security principles a requirement. We, as citizens, businesses, and the state government, must continue to focus on the protection of our consumers and national security.

In a recent statement, the President insisted that the private sector needs to take immediate action to improve its defenses against likely cyberthreats. This is the most recent and urgent caution we have seen yet, following a string of regular notices to implement robust cybersecurity procedures since the fall of 2021. As a practitioner in the field of cyber security, I believe that the President's statement is a warning that the US government may have specific intelligence requiring our complete attention and focus on reducing the threat of cyber intrusion.

Reclamere partners with several industry leaders to support our client's information security needs. One of the leading international service providers recently shared that their 24/7 threat operations center "has seen no noticeable increase or sophistication in the volume of attacks while monitoring our customer base, we strongly recommend all our partners to treat this latest statement as a call to action to harden your infrastructure and verify that cyber hygiene best practices are being followed. As a start, review the controls and benchmarks provided by the Center for Internet Security (CIS)."

Recommendations to Improve Cybersecurity Resiliency

Whether an organization is a state government, healthcare, insurance, financial services provider, or an educational institution we strongly recommend the following actions be taken before the end of 2022.

1. Identify a cybersecurity resource that has the demonstrated experience to develop, conduct, and report the findings of an enterprise-wide information security risk assessment. This will allow the organization to see a snapshot in time of the current risk profile and the areas for immediate, short-term, and long-term improvement.

2. The risk assessment must deliver a risk action plan that will help the organization to risk rank and prioritize the steps necessary to improve the cyber resiliency of the organization. The plan needs to be practical, meaningful, and actionable.

3. Develop a remediation strategy as a follow-on activity to the risk action plan. Decide on what resources will be necessary to achieve the strategy, whether those are internal or with a trusted third-party partner.

4. Meet with your current or potential cyber insurance carrier to determine how best they can assist the organization with risk management.

Additionally, I encourage all of us to accept some basic facts about information security. The information that we want to create and have access to has an incredible value to cybercriminals. Cybercriminals are getting smarter and working harder every day. Complete and 100% data security is not a reality. Do not let these facts discourage you, but rather be a wake-up call that says, we must act now. If the four items that were just mentioned seem too much or far off in your organization then at least do one thing very well – train your employees about cyber resiliency and hygiene and consider rewarding them for protecting your most valuable asset – digital data. Employees are the first line of defense in all organizations and making sure they understand, appreciate, and can combat outside threats is essential in protecting data. These training programs need to be ongoing, challenging and based on the risk profile of employees. We do not all view risk in the same way, so delivering training that mirrors the risk profile of the individual is key to helping them protect you.

In conclusion, we must accept the reality that for our schools, businesses, and government to develop strong cyber resiliency it will be an ongoing journey and not a check box that we are done. The senior leadership ranks must make their organization's information security risk posture a part of their overall strategy and budget. Identifying and partnering with qualified and experienced trusted third-party managed security service providers is essential to winning the long game in this cyber battle.

The challenges brought about by cyber-attacks are a global problem, therefore we must continue to leverage and maximize resources whenever possible to understand and detect persistent threats. I strongly encourage this committee to identify Pennsylvania information security practitioners to collaborate on practical solutions to this immediate problem. Additionally, this committee should bring together both state and national law enforcement resources to collaborate with information security practitioners. This collaboration should also involve the review and development of any current or future legislation pertaining to the subject of data breaches. In the area of legislation, I caution you to avoid a "one size fits all" model that could be impossible to attain for small organizations, nonprofits, and education. Established tiers of responsibility and compliance levels may better serve all while legislating a single set of standards that can be embraced and addressed successfully.

Finally, let me again express my appreciation for this opportunity to present written testimony to this committee. Your jobs are not easy, there are not limitless resources available to solve this problem, and the bad actors are not going away. Please know that there are companies like Reclamere here in Pennsylvania with decades of experience, the resources to help solve this problem, and a desire to help you as you develop future legislation. I encourage you to develop that public / private partnership to minimize the damages created by cyber-attacks. This is a battle worth fighting and one that the private sector is willing to help you win. Thank you and I would be able to answer any questions that you may have.

Respectfully Submitted,

Joseph P. Harford, Ph.D., CSDS
Founder and President
Reclamere, Inc.
814-599-0242
joseph@reclamere.com