Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

Testimony to the Pennsylvania House Republican Policy Committee
March 28, 2022

Over the past year the world has borne witness to a burgeoning cybercrime economy and the rapid rise of cybercrime services. We have watched this global market grow in both complexity and fervency. We've seen the cyberattack landscape becoming increasingly sophisticated as cybercriminals continue—and even escalate—their activity in times of crisis. New levels of supply chain and ransomware attacks were a powerful reminder that we must all work together, and in new ways, to protect the cybersecurity of the planet.

Microsoft serves billions of customers globally, allowing us to aggregate security data from a broad and diverse spectrum of companies, organizations, and consumers. Informed by over 24 trillion security signals per day, our unique position helps us generate a high-fidelity picture of the current state of cybersecurity, including indicators that help us predict what attackers will do next. Each year we prepare the Microsoft Digital Defense Report, which brings together integrated data and insights from across our teams. By compiling and sharing the report we aim to help the global community strengthen the defense of the digital ecosystem, and provide actionable learnings that companies, governments, and consumers can use to further secure individuals and environments.

Cybersecurity trends identified in the Digital Defense Report

As pointed out in this year's report, there is a growing threat of cybercrime as cybercriminals target and attack all sectors of critical infrastructure; ransomware attacks are increasingly successful, and the profits from these are soaring; and the cybercrime supply chain, often created by criminal syndicates, continues to mature as well. Almost anyone can buy services needed to conduct malicious activity.

It used to be that cybercriminals had to develop all the technology for their attacks. Now, in this rapidly developing cybercrime economy they can rely on a mature supply chain, where specialists create cybercrime kits and services that other actors then buy and incorporate into their campaigns. Over the past 12 months, we've seen that the number of sites offering services has significantly increased, as well as volume of stolen credentials and variety of phishing kits.

Governments can mitigate cyber threats

Despite the challenges, we do see hope for governments. First, more governments and companies are coming forward when they are victims. This transparency has made clear to governments around the

world that cybercrime is a threat to security. Victim stories help to humanize the problem and make clear the consequences of those attacks, and, in drawing attention to the problem, we're seeing more engagement from incident responders and law enforcement.

Second, now that governments around the world recognize that cybercrime is a threat to national security, they've made combatting it a priority. Governments are passing new laws regarding reporting, they're creating cross-government task forces, allocating more resources, and seeking out private sector partnerships.

With increasing threats, even with increased sophistication, basic security hygiene still protects against 98% of attacks. Good cybersecurity hygiene includes:

- Enabling and consistently using multi-factor authentication
- Applying the concept of "least privilege" when granting access to information and technology resources
- Utilizing antimalware tools
- Keeping software versions up-to-date

The key actionable learning from all the elements of this report is that to minimize impact of attacks we must truly practice good cyber hygiene, implement architectures that support the principles of Zero Trust, and ensure cyber risk management is integrated into every aspect of the business.

What governments can do now

As we increasingly do more of our work online, so do criminals and nation state attackers. Governments must take this realization into consideration as they plan digital activities. For any new venture, consider the threat alongside the opportunity, and think about how you can manage risk for your entire organization.

This kind of thinking will require fundamental changes in the way we operate. We must consider risk as a whole and across the organization, rather than within siloes or individual viewpoints. We must look at where we need to change the way we work, and where we need to do the things we are already doing—but better. We encourage you to consider the following as you think about improving your security posture:

- Do the basics well. Although attackers are becoming more sophisticated, good cyber hygiene and implementation of basic security measures is often the best way to disrupt, prevent, and detect their attacks.

- Take a holistic view. Too often the way we organize security and risk is driven by our own organizational structure and siloes. Attackers will look for vulnerabilities across these siloes, so we need to consider risk and the best approach to mitigating risk at an organizational level. This may require some standardization or translation of approaches across the different teams in an organization. It also underlines the importance of standards as we seek to harmonize between

companies, which is increasingly important to managing supply chain risk.

- Any element can be used as an attack vector. Attackers will look for the weakest link across an organization's ecosystem, so we must manage it holistically. The weakest link may be a connected freezer or building management system that is used to gain access to the network, or it may be a user or device that is compromised via a phishing email in an attempt to gain access to the operational technology running a factory or production plant. We need to consider and manage the organization's entire attack surface.

- Think about people. People engage with technology and can be used as a way of gaining access to the digital environment. Think about how to engage with them in a way that will help them to understand the risks they face. Understanding, engaging, and educating people will allow them to become a key line of defense against modern threats, whether that is misinformation seeking to influence peoples' decisions and undermine democracy or phishing emails seeking to gain access to and compromise an organization's digital assets.

- Zero Trust is an architectural principle. The threats we have seen underline the importance of Zero Trust in designing and managing the risk in an organization. The last year has emphasized why there should be no such thing as a trusted application, trusted user, or trusted device with unrestricted access. The risk and context of every connection needs to be considered before allowing access to resources. Zero Trust is not a technology but an approach to managing risk. When implemented properly, it can enable us to unlock the potential of modern technology while limiting our exposure in a hyperconnected world.

Addressing the cybersecurity talent pipeline

Making technical improvements is critical, but alone is not sufficient to stop the threats facing our state and country. Governments, like private companies, struggle to recruit and retain qualified cybersecurity professionals. We need to solve the cyber talent pipeline.

Annually only 3% or roughly 65,000 of US students are securing a credential in computer and information sciences, and far fewer are specializing in cybersecurity. At the same time, recent analysis from LinkedIn and Cyberseek.org shows that there are nearly 500,000 job openings in cybersecurity today. These are great jobs that pay an average of $105,800 per year. And students can qualify for many of these open jobs by earning an industry-recognized certificate or by getting a certificate or associates degree from a community college.

We believe community colleges are the single greatest potential asset the United States has in expanding the cybersecurity workforce. That's why Microsoft has launched a national campaign with US community colleges to help skill and recruit into the cybersecurity workforce 250,000 people by 2025, representing half of the country's workforce shortage.

Building on our Skills for Jobs initiative, we are extending our programs, partnerships and investments.

Our initial commitment will make curriculum available free of charge to all of the nation's public community colleges, provide training for new and existing faculty at 150 community colleges, and provide scholarships and support services to 25,000 students, 10,000 at community colleges.

The nation's cybersecurity workforce is notably lacking in diversity, with 82.4 percent of the country's cybersecurity jobs currently held by men and 80 percent held by people who are white. We need to build a cybersecurity workforce that is both larger and more diverse. Community colleges are uniquely situated to help do both.

Through partnerships with the American Association of Community Colleges, National Cybersecurity Training & Education Center (NCyTE) and Last Mile Education Fund, we offer:

- Faculty professional development and support for earning Center of Academic Excellence in Cyber Defense Designation
- Community of practice to support expanding cybersecurity programs
- Scholarships for low-income students – including Veterans - pursuing cybersecurity career pathways
- Ready-to-teach curriculum and teaching materials aligned to industry needs

Additional resources
Digital Defense Report (http://aka.ms/mddr)
Community College Cyber Skilling Initiative (http://aka.ms/cyberskills)
Skills for Jobs Initiative (https://opportunity.linkedin.com/)

Contacts for the Commonwealth of Pennsylvania

Tyler Clark
State Government Affairs Industry manager
tylerclark@microsoft.com

Michael Mattmiller
State Government Affairs Industry Lead
mimattmi@microsoft.com

Jay Summerson
State Government Affairs Senior Director
jay.summerson@microsoft.com