Testimony of Eunice Santos

Before the

House Oversight and Government Affairs Committee
Subcommittee on Information Technology

Federal Efforts to Improve Cybersecurity

June 20th, 2016
Chicago, Illinois

Chairman Hurd, Ranking Member Kelly and Distinguished Members of Congress, I appreciate the opportunity to provide testimony to the Subcommittee at today's field hearing.

By way of background, I am the Ron Hochsprung Endowed Chair and Professor in the Department of Computer Science at Illinois Institute of Technology (Illinois Tech) and also serve as the Chair of the Department. My work focuses on large-scale parallel and distributed processing, computational modeling, cybersecurity, cloud computing, complex adaptive systems, and human modeling with applications to the biological, physical, and social sciences. Among other past endeavors, I served as a Senior Research Fellow at the US Department of Defense's Center for Technology and National Security Policy.

Illinois Tech is a private, technology-focused, research university offering undergraduate and graduate degrees in engineering, science, architecture, business, design, human sciences, applied technology, and law. One of 21 institutions that comprise the Association of Independent Technological Universities (AITU), Illinois Tech offers exceptional preparation for professions that require technological sophistication, an innovative mindset, and an entrepreneurial spirit. The university commitment to diversity is reflected in its policies and its global student enrollment.[1]

Illinois Tech is also designated as a National Center of Academic Excellence in Information Assurance by the National Security Agency and the Department of Homeland Security.

[1] https://web.iit.edu/about/quick-facts

My testimony will focus on several aspects of the cybersecurity challenge facing this country, including (1) the threats faced by educational institutions in protecting against data breaches, (2) the role of higher education institutions in developing the cybersecurity workforce of the future, and (3) research-informed considerations that can help the Federal government in its efforts to effectively address cybersecurity.

I. The Challenge Facing Institutions of Higher Education.

Institutions of higher education face a wide variety of cyber-threats. A typical university will have extensive personnel and payroll data, privacy-protected student information (including Social Security numbers), and extensive financial aid information. In addition, a research university will host extensive research and informational databases – including highly sensitive research information that may include human subjects information, as well as high value intellectual property.

Along with the threat of compromising sensitive data, higher education institutions are similar to many other organizations in that they are vulnerable to suffering system downtime and expense related to cyber-attacks, damage caused by malware, expense related to ransomware, and the compromising of sensitive data.

At Illinois Tech, cyber-attacks occur constantly. As noted by our IT personnel, among other types of incidents, this includes malware, phishing attempts, and hacking to access computational resources or data. In some cases, the attacks are not particularly sophisticated and they are blocked by our staff and existing systems. Unfortunately, the challenge with cybersecurity is that the threats are ever-evolving, with new methods of attack developed every day. The risk is always what you do not know and therefore cannot protect against.

Like many organizations, Illinois Tech has deployed the majority of the currently available industry tools, such as virus protection, firewalls, intrusion detection and intrusion-prevention systems and more. Pursuant to the ever-evolving nature of the threat, improving our security is work that never stops. We must constantly continue our efforts to enhance our security capabilities.

The Committee should be aware of some of the unique aspects of non-profit and public higher education institutions that make the cybersecurity challenge more daunting. Such institutions need to have an open technology environment in order to support their academic mission and the needs of students and faculty. Research universities must support their investigators' often unique technology configuration requests in order to enable their scientific efforts. As a consequence, universities typically have multiple operating systems that are used by faculty and staff in various departments and settings. Some departments will have their own domains. This has a variety of management consequences. For example, in such a heterogeneous environment, more personnel, training and virus protections are required.

Universities also must support potentially tens of thousands of users in a "Bring Your Own Device" (BYOD) environment. This leads to extensive user autonomy with regard to applications, technologies and file sharing. Unfortunately, with such autonomy comes increased risk of malware, ransomware and the like. Additionally, most universities must have international connections that often rule out the use of geo-location blocking approaches.

This level of diversity and porousness in a university's IT environment can make the provision of staffing, monitoring and other support more complex. This is less of a problem for corporations, partnerships and similar organizations that have more ability to create a "top-down" unified IT structure. It also necessitates a defensive approach that prioritizes protection of the most sensitive data and systems.

Developing university-specific repositories that collect information in a systematic manner on the events and lessons learned in managing these threats would provide substantial knowledge that can be used in case-studies, education and training. However, cross-sharing of such information among universities presents certain challenges, including how to exchange specific institutional information, and how to maintain privacy protections.

II. Building the Cybersecurity Workforce of the Future.

Illinois Tech is at the forefront of cyber education. As mentioned, the University is designated as a National Center of Academic Excellence in Information Assurance by the National Security

Agency and the Department of Homeland Security. The centers of gravity for our efforts in these areas are the Computer Science Department within the College of Sciences and our Information Technology and Management (ITM) programs within the College of Applied Sciences.

Cybersecurity is a core research and education area within the Department of Computer Science. Both undergraduate and graduate students are offered coursework that will educate them on the issues and advances in cybersecurity, including:[2]

(a) Undergraduate students are offered coursework that educates them on encryption systems, operating system security, database security, network security, system threats and risk avoidance procedures. Additionally, they are educated on the algorithms and techniques used to defend against malicious software.

(b) Graduate students are offered training in the theory and practice of cryptography and network security. Students who wish to pursue careers focused on real-world security issues or research can take advanced courses that provide a thorough grounding in cyber-security issues. This includes semester-long research projects and study regarding how to address issues such as unwanted traffic (e.g., denial of service and spam); malware; network configuration and defense; and cyber physical system security (e.g. critical infrastructure protection).

The Department of Computer Science also hosts extensive research activities, including cutting edge work on cyber security research. In particular, our faculty have research foci in forensic linguistics, cyber-trust and suspicion, and trustworthy cyber-physical critical infrastructure.

At both our Chicago and Wheaton, campuses, our Information and Technology Management programs offer education at the undergraduate and Masters levels in cyber forensics, and network security.

These programs are supported by the School of Applied Technology's Cyber Forensics and Security Laboratory (ForSec Lab). The lab provides students and research partners the

[2] http://science.iit.edu/computer-science/programs/course-descriptions

opportunity to develop hands-on expertise working in the field of security, forensics, and disaster/data recovery. This type of cyber security and forensics research, testing and analysis benefits both academic and industry organizations. It provides an environment where traffic throughout a network can be analyzed and filtered. Cyber intrusions and virus spread can be studied, as well as Malware and Spyware can be tested on multiple platforms. [3]

Finally, Illinois Tech has also established the Center for Cyber Security and Forensics Education C²SAFE. The Center exists to fulfill several missions, including (1) promoting education and research in cyber security technologies and management, information assurance, and digital forensics across all academic disciplines; (2) engaging with business and industry, government, professional associations, and community colleges; (3) coordinating our designation as a National Center of Academic Excellence in Information; and (4) publishing student and faculty research and sponsoring conferences and other events.[4]

Illinois Tech has provided many different avenues for education, training and research in the field of cybersecurity. Our computer science students are in high demand and work in a variety of sectors including tech, health, finance, research, entertainment, education, government and others. With the ubiquitousness of technology, the sectors that do not need to actively and seriously consider effective cybersecurity methods are few and far between.

III. The Need to Address the Social and Organizational Dimension.

The Federal government has stepped up to address the challenge of cybersecurity through legislation such as the Cybersecurity Act of 2015, the President's Cybersecurity National Action Plan, appropriations to myriad agencies to improve systems and tactics, and various efforts with critical industry sectors.

As mentioned above, cyber-threats are ever evolving. One area in which I would like to encourage greater focus is in understanding the social and organizational dimension of threats; in particular, how human beings knowingly or unknowingly compromise security and what can be done about that. I believe that more research in this area can produce dividends in terms of better understanding how individuals respond in the cyber world to inputs that can compromise

[3] https://appliedtech.iit.edu/cyber-forensics-security/about/overview
[4] https://appliedtech.iit.edu/c2safe/mission-purpose

security. For example, improved understanding of what are major drivers for why certain individuals may be unduly influenced or inappropriately trust cyber-communication requests rather than becoming suspicious, and what are the environmental/cultural issues within an organization that can allow certain security issues to flourish. By better understanding these aspects of human behavior, we can develop improved public education, employee training approaches, and refine procedures and policies to produce improved outcomes and mitigate risks.

Thank you very much for this opportunity to testify. I would be pleased to answer any questions you may have.