08 NOV 2017

FUNDACÃO CALOUSTE GULBENKIAN
LISBOA / PORTUGAL

Keynote Speeches Summary

Conference “Innovation Meets Cybersecurity”

8 november 2017 – Fundação Calouste Gulbenkian, Lisbon

Suzanne Spaulding

“Global Innovation Networks: Making the Business Case for Cybersecurity"

Digital Innovation and Cybersecurity

Cybersecurity is not the goal. The goal is to be able to enjoy all the benefits that a networked world has to offer. Along with those benefits, an increasingly connected world brings new risks, which must be appropriately managed. Political support for smart cities will falter if cyber incidents threaten privacy or safety. Consumers will think twice about smart homes if they turn out to be exploited by criminals. And industry will question the value of interconnected machines if cyber-enabled malfunctions harm customers or damage business operations. Appropriate cybersecurity thus enables digital innovation.

Managing cyber risks requires that you assess those risks, looking at threat, vulnerabilities, and consequences, and then determine ways to mitigate against all three. Cybersecurity traditionally has focused heavily on threats and vulnerabilities. Not nearly enough attention has been paid to understanding and mitigating consequences, although this is often the most useful place for companies to begin their risk assessment. Prioritizing efforts is key to effective cybersecurity, and understanding impacts of cyber incidents is key to that prioritization. This requires an enterprise-wide approach that considers the entire value chain. Managing cyber risks is not just an IT problem.

If we take an effective risk management approach to the Internet of Things, finding ways to bring cybersecurity providers and the IoT builders together, we can significantly enhance the cybersecurity of the Internet. The number of devices coming online will rapidly dwarf the existing, insecure online environment. If we get this right, IoT can be part of the solution rather than just a massive attack surface.

Donna Dodson

"Governance of Public-Private Cooperation: Progress and Challenges"

Innovations and Cybersecurity – Roles for the Private and Public Sectors

Awareness about the importance of strong cybersecurity for maintaining trust in the economy is at an all-time high in many nations. Today's digital infrastructure is an economic engine but there still remain questions on how to protect the infrastructure. Donna Dodson will discuss investments in today's cybersecurity best practices to support tomorrow's innovations. She will describe current and future activities that build on today's partnerships in the private, academic and public sectors. In addition, she will describe the National Institute of Standards and Technology (NIST) current path-breaking research and development and its work to cultivate standards and best practices, and facilitate technology transitions.

Tim Maurer

"Toward a Global Norm Against Manipulating the Integrity of Financial Data"

The financial crisis that erupted in 2007 highlighted how important trust is for the global system and how fragile it can be. The 2016 Bangladesh central bank cyber incident exposed a new threat to financial stability and the unprecedented scale of the risk that malicious cyber actors pose to financial institutions. While financial institutions have been targeted by hackers since the early days of the modern Internet, the threat has evolved and grown. In 1995, for example, hackers stole USD 10 million from a major bank at a time when most people were just starting to connect to the Internet. Cybercrime has since increased to the billions. The Carbanak group reportedly stole USD 1 billion over the course of a few years. Importantly, politically motivated actors have been carrying out increasingly risky actions in

recent years. It is therefore no surprise that G20 Finance Ministers and Central Bank Governors are becoming increasingly alarmed by this evolving threat.

In their March 2017 communiqué, the G20 Finance Ministers and Central Bank Governors warned that "The malicious use of Information and Communication Technologies could …undermine security and confidence and endanger financial stability." That is why, the Carnegie Endowment has proposed that the G20 explicitly commit not to engage in offensive cyber operations that could undermine financial stability, namely manipulating the integrity of data of financial institutions or undermining the availability of critical systems, and to cooperate when such incidents occur. Such an agreement by the world's leading economies would send a clear signal condemning such activity and enable future cooperation. The G20 has been discussing such a commitment by its member states, which, if adopted, will require the collaboration between governments, financial institutions, and technical experts to be effective.

More details are available at www.protectingfinancialstability.org