TIM Lecture Series
The Expanding Cybersecurity Threat

Cheri F. McGuire

> *"It used to be that not a month would go by without some new data breach being reported. Then it seemed not a week would go by. Today, we see daily reports about some new attack vector, some new cyber-espionage group, some new kind of cyber-attack occurring against our critical networks and our critical data."*
>
> Cheri F. McGuire
> Vice President of Global Government Affairs & Cybersecurity Policy
> Symantec

Overview

The TIM Lecture Series is hosted by the Technology Innovation Management program (carleton.ca/tim) at Carleton University in Ottawa, Canada. The lectures provide a forum to promote the transfer of knowledge between university research to technology company executives and entrepreneurs as well as research and development personnel. Readers are encouraged to share related insights or provide feedback on the presentation or the TIM Lecture Series, including recommendations of future speakers.

The first TIM lecture of 2015 was held at Carleton University on February 19th, and was presented by Cheri F. McGuire, Vice President of Global Government Affairs & Cybersecurity Policy at Symantec (symantec.com). McGuire provided an overview of Symantec's view of the expanding cybersecurity threat and the measures the company is employing to mitigate the risk for companies and individuals. The slides from her presentation are available here (tinyurl.com/m63vk7t).

Summary

To begin, McGuire provided background on Symantec's systems for identifying and evaluating cyber-threats around the world, which it uses as a basis for developing protection measures. In particular, she described Symantec's Global Intelligence Network (GIN), a massive array of monitoring systems, attack sensors, and decoy accounts, combined with the world's largest vulnerability database and capability for big data analytics, which together provide real-time insights on what is happening on a global scale.

Globally, a wide range of threats are being detected across many platforms and devices. There is also wide range of attackers, from highly-organized criminal enterprises to individual cyber-criminals to "hacktivists" (i.e., politically motivated actors) to state-sponsored groups. The variety of threats and motivations make Symantec's task of identifying threats and developing protections an increasing challenge and drives its focus on the attackers' tactics, techniques, and procedures (TTP). A detailed understanding of the attackers is essential in building effective defenses against them.

Today, the key categories of threats raised by attackers are:

1. Data breaches: more than 550 million identities were exposed due to data breaches in 2013, and Symantec expects this number to soon exceed 1 billion, which is equivalent to nearly 1 out of every 7 people on the planet, or about 1 in 3 Internet users. And, data breaches are becoming increasingly broad: intellectual property, trade agreements, and business agreements, are often now the target, not just credit card data, etc.

2. Mobile and social: a key area where threats are proliferating and where social engineering is carried out (i.e., attackers gather personal data about persons of interest via social networks and then use it to make targeted emails more convincing).

3. Ransomware: malware that locks a computer and encrypts the data, then demands payment for decryption. Ransomware is becoming increasingly prevalent: Symantec observed a 500% month-on-month increase in ransomware in 2013.

TIM Lecture Series – The Expanding Cybersecurity Threat

Cheri F. McGuire

4. Cyber-espionage: the identity of malicious intruders is not always known, and the distinctions between categories of attackers is not clear-cut: one group may pose as another to obscure their identities and intentions, particularly when the attacks are initiated by nation-states.

5. Internet of Things: innovation in this area is happening very quickly, but the security is a step behind. Symantec believes that, to be effective, security must be built into products as they are being developed, not "bolted on" later.

In terms of targets, McGuire highlighted critical infrastructure (e.g., power grids, transportation networks, manufacturing sectors, financial systems) as an important area of concern.

McGuire also highlighted the increase in web-based attacks: in 2013, Symantec blocked 23% more web attacks than in 2012. However, targeted attacks are of particular concern, such as emails targeted at persons of interest using personal data gathered to increase the apparent authenticity of the communication. Such targeted emails are designed to trick people into taking actions that they would not otherwise take if they understood the consequences. Examples include spearphishing (i.e., sending an email to a person of interest) and watering holes (i.e., drawing targets to infected websites, where the malware lies waiting to infect visitors).

Beyond Symantec's efforts to develop its products and services, the company has also been actively pursuing public–private partnerships to help counter the expanding cybersecurity threat. These partnerships are both private-to-private and private-to-public; Symantec is working with other companies and with many government agencies that span policy, operations, law enforcement, as well as education and awareness. Such partnerships are motivated by the desire to cooperate and share high-level information, support prosecutions of cyber-crimes, and develop an ecosystem approach to cybersecurity. This approach also reflects the shift towards a defense that is not solely founded on signature-based technologies (i.e., antivirus software), but reflects an increasingly sophisticated, layered approach to cybersecurity.

Finally, McGuire provided a list of best practices for businesses to help protect against cyber-threats:

1. Employ defence-in-depth strategies
2. Monitor for network incursion attempts and vulnerabilities
3. Antivirus on endpoints is not enough
4. Secure websites against man-in-the-middle attacks
5. Protect private keys
6. Use encryption to protect sensitive data
7. Ensure all devices on company networks have security protections
8. Implement a removable media policy
9. Be aggressive with updating and patching
10. Enforce an effective password policy
11. Ensure regular backups are available
12. Restrict email attachments
13. Ensure an infection and incident response procedure is in place
14. Educate users on basic security protocols

TIM Lecture Series – The Expanding Cybersecurity Threat

Cheri F. McGuire

About the Speaker

Cheri McGuire is Vice President for Global Government Affairs and Cybersecurity Policy at Symantec, where she is responsible for the global public policy agenda and government engagement strategy, which includes cybersecurity, data integrity, critical infrastructure protection, and privacy. She currently serves on the World Economic Forum Global Agenda Council on Cybersecurity, and on the boards of the Information Technology Industry Council, the US Information Technology Office in China, and the National Cyber Security Alliance. She also is a past board member of the IT Information Sharing and Analysis Center, a former member of the Industry Executive Subcommittee of the President's National Security Telecommunications Advisory Committee, and a former Chair of the US IT Sector Coordinating Council. Ms. McGuire is a frequent presenter on technology policy issues, including testifying five times before the US Congress on cybersecurity, privacy, and cybercrime. Prior to joining Symantec, she served as Director for Critical Infrastructure and Cybersecurity in Microsoft's Trustworthy Computing Group, and she has held numerous positions in the Department of Homeland Security, Booz Allen Hamilton, and a telecom engineering firm that was acquired by Exelon Infrastructure Services. She was also a Congressional staffer for seven years. Ms. McGuire holds an MBA from The George Washington University and a BA from the University of California, Riverside.

This report was written by Chris McPhee.

Citation: McGuire, C. F. 2015. TIM Lecture Series – The Expanding Cybersecurity Threat. *Technology Innovation Management Review*, 5(3): 46–48.
http://timreview.ca/article/881

Keywords: cybersecurity, cyber-attacks, cyber-threats, data breaches, cyber-espionage, social engineering, malware, ransomware, scareware, antivirus, private-public partnerships, Symantec