TIM Lecture Series
The Business of Cybersecurity

David Grau and Charles Kennedy

> *"Fundamentally, the key problem in cybersecurity isn't the technology – it's a people problem."*
>
> David Grau
> Head of Threat Response, TD Bank Group

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 third TIM lecture of 2014 was held at Carleton University on March 26th, and was presented by David Grau, Vice President and Head of Threat Response, Intelligence, and Defensive Technologies at TD Bank Group (td.com), and Charles Kennedy, VP Credit Card Technology. Kennedy and Grau discussed the state of the information security industry and current trends in threat management and focused their lecture on the banking industry and the TD Bank Group's experience with cybersecurity within it. However, many of the messages are applicable to broader and multidisciplinary domains.

Summary

The lecture began with an overview of the state of the industry, including types of common threats faced today, such as malware, physical attacks, social engineering, social media, misuse, errors, and environmental effects. Kennedy highlighted that hacking is a particular priority that disproportionately introduces risk to the bank and its customers. Hacking can take the form of system hacking (e.g., operating systems), infrastructure hacking (e.g., wireless, hardware, network devices), or application and data hacking (e.g., ports, code, users). Typically, events that occur as a result of these types of activities are not a case of one individual criminal targeting an individual user; more common and significant threats come from automated systems.

These threats are not perceived in the same way by all people or organizations. Kennedy explained that the degree and nature of concerns – or posture – in relation cybersecurity threats varies between citizens, governments, and infrastructure organizations:

1. **Citizens** are typically worried about identity protection and identity theft, social networks, convenience, privacy, confidentiality, and issues relating to mobile (e.g., payments, reservations, location, retail applications). In this group, the typical demographics point to high rates of use and adoption of the Internet and mobile technologies among young adults.

2. **Governments** are typically worried about data protection and theft, as well as the reliability of both the public and private sectors. The concerns of individual governments may be unique, and there is a wide range of postures around the globe. Initial steps are being taken to define the international rules of engagement for governments combating cyberterrorism and cyberwarfare. Examples include *The Talinn Manual on the International Law Applicable to Cyber Warfare* (NATO, 2013; ccdcoe.org/249.html)

3. **Banks and key infrastructure** are typically worried about maintaining financial services (e.g., payments and exchanges), utilities, and commercial activities. Innovation, research, and response all depend upon co-operation between industries and between gov-

The Business of Cybersecurity

David Grau and Charles Kennedy

ernment and industry. The increasing complexity of the threats necessitates increasing co-operation in the future.

Threat actors and motivations

Grau highlighted the natural tendency of information security staff – as technologists – to look at problems from a technology perspective. When evaluating a security threat or incident, this tendency leads to a focus on the tangibles – the what, the when, and the where – that can be analyzed and processed. Often, this analysis comes at the expense of considering the human element – the who and the why – and leads to the creation of tools that reinforce the technology bias, and leaves staff overwhelmed with a massive and increasing volume of unmanageable data. In response to the current state of affairs in information security, much greater attention must be paid to the factors that motivate actors. Unless efforts are focused on indentifying and understanding the who and the why, there is insufficient context to detect the important patterns in large volumes of event data and to make intelligent decisions based on that data.

Broadly speaking, the threats facing citizens, governments, and infrastructure organizations come from three types of actor:

1. **The Criminal:** motivated by profit; focused on fraud; the "top of the food chain"

2. **The Hactivist:** motivated by sociopolitical causes; focused on drawing attention through disruption and shaming; adopts tools and methods from criminal actors; examples: Anonymous, AntiSec.

3. **The Nation-State:** motivated by political or economic advantage; focused on espionage; late adopters that learn from criminal actors and hactivists

Of these three types of actors, criminal actors are the greatest concern in the banking industry, and so the greater part of the lecture focused on describing the threats posed by criminal actors and the bank's strategies to not only defend against them, but take proactive steps to reduce the risk they pose. The threat levels from the other two types of actor are increasing; however, criminal actors remain the greatest threat to the banking industry, in part because of their profit motive, but also because most of the innovation tends to come from this group – the hactivist and nation-state actors typically adopt the techniques and technologies that were first developed by the criminal actors.

Compared to just 15 years ago, the criminal landscape has changed considerably. Whereas criminal activity in cyberspace was typically initiated by "one-man shows", there are now complex criminal ecosystems that are both stratified and service oriented. For example, the tiers of actors in an ecosystem might include the following:

1. funders (e.g., organized crime)
2. malware writers
3. botnet operators
4. botnet users
5. money mules (i.e., those who transfer money out of the ecosystem)
6. mule herders (i.e., those who line up the connections to money mules)
7. state-funded "skunkworks"

In the past, security efforts might have targeted the individual who writes the malicious code, who likely also would have played all or most of the roles listed above. Now, the servitization of the criminal ecosystem means that actors wishing to commit fraud do not require advanced technical skills; the required tools and services are readily available and easy to use. However, once the fraud has been committed, it remains a challenge for the criminal actors to retrieve the money. As the people who take the money out of the ecosystem, the money mules are the weakest link in the chain – the most likely to be detected and the most likely starting point for further investigation of the ecosystem. To illustrate the sophistication and stratification of the criminal ecosystems, Grau provided examples of services offered within such networks, such as fraud aggregators, which are websites that collect and organize stolen data (e.g., credit card numbers), which can then be queried by criminal actors.

Current and emerging trends

Grau examined some of the current and emerging trends in techniques used by threat actors, including:

1. **Man-in-the-browser attacks:** a method of using malware to create a false, but truly convincing, browser experience to a victim and to harvest credentials and other valuable data in the background. This type of malware is fully automated, easy to use, and very powerful. Because it is so convincing – even the URLs in the browser address bar appear correct – this type of approach is much more effective than traditional phishing techniques. It is also very difficult to detect with anti-virus and anti-spyware applications, and so there is an urgent need for innovation in this area.

The Business of Cybersecurity

David Grau and Charles Kennedy

2. **Ransomware:** malware that installs itself on a computer and pretends to be anti-virus or other well-intentioned software. For example, it may present the user with a choice of whether or not to allow the software to "clean" the computer, but if the user declines, it either permanently damages the victim's hard drive or demands online ransom payments.

3. **Polymorphism:** malware that is customized to each user, meaning that each version of the malware is unique to that user even if it may be functionally identical to another version. This approach can overcome the types of general rules and definition databases that traditional anti-virus software depend upon.

4. **Packaged exploit kits:** malware frameworks that deliver tailored packages of malware components that correspond to a victim's particular vulnerabilities. If a user can be tricked into visiting a website where a packaged exploit kit is installed, the framework tests the victim's computer and then packages a set of exploits designed specifically to suit the victim's vulnerabilities. This customized approach also means that the criminal actors do not need to "show all of their cards" in terms of the full complement of exploits they have available. This approach can also take advantage of polymorphism to obfuscate the new, customized package.

5. **Distributed denial-of-service attacks (DDoS):** an approach that effectively creates a massive digital traffic jam in the target organization's infrastructure, usually by amplifying and redirecting traffic to the target's network. Although in the past, DDoS attacks were typically "nuisance" attacks, this approach is now often used as a diversionary tactic to facilitate fraud.

6. **New-generation botnets:** networks of computers under an outside actor's control for the purposes of sending spam or participating in DDoS attacks. In the past, botnets primarily recruited thousands of individual home computers; however, the scale of the botnet approach has grown massively not by increased recruitment of additional computers, but by focusing on servers, which provide much greater power per infection, resulting in smaller but more powerful botnets that can have enormous disruptive potential.

In describing current and emerging threats, Grau cautioned that the term "advanced persistent threat", or APT, is often misused and overused, because all modern malware is advanced, is persistent, and is a threat, in addition to being sophisticated, stealthy, and evasive. A true APT shares all of these characteristics, but it is also rare, targeted, customized, and attributable (i.e., not opportunistic).

Unfortunately, traditional anti-virus software is largely ineffective against the current and emerging techniques used by criminal actors. Verizon (2011; tinyurl.com/lvdpsnl) reported a 37% success rate for anti-virus applications in its study of data breaches; other datasets report even lower numbers. The key reason is the growing complexity of the problem: as additional devices and features appear, the attack surface grows. As more and more ways appear for criminal actors to infiltrate a system, it becomes increasingly difficult to protect the entire attack surface. Grau provided several industry examples, including the Zeus Trojan horse and Cryptolocker ransomware, and the 2013 Target data breach, to reinforce the sophistication of current and emerging threats.

Innovation opportunities

Based on their experiences, Grau and Kennedy identified the following areas where innovation is needed in the cybersecurity domain:

1. **Skilled workers and innovators:** there is a shortage of talent in the information security domain.

2. **Borderless networks:** organizations no longer have a well-defined perimeter – this paradigm has become outdated. Today, organizations are more porous and no longer have clearly defined "doors" that simply need to be locked down by security staff. There is now a need for ubiquitous security (e.g., a portable security stack) that does not just assume a defensive posture, but is nimble, pervasive, and dynamic.

3. **Avoiding fragmentation of the Internet:** changes to the Internet over time in response to the cybersecurity threats provides incentive for nations to fragment the Internet (e.g., the Great Firewall of China). The underlying problem is that efforts to enhance cybersecurity are often at odds with the ideals upon which the Internet is based and requires to function effectively.

The Business of Cybersecurity

David Grau and Charles Kennedy

4. **Security as big data analytics:** there is a need for real-time detection of events with in-line correlation and decision making based on scores derived from analytics.

5. **Wetware versus software:** there is a mismatch between the data experts, who do not understand the threat scenarios, and the security professionals, who do not understand the data analyses.

6. **Intelligence gap**: threat intelligence is extremely valuable – it helps focus efforts and greatly increases the speed of response. There is a need for tools and processes that allow more mature intelligence analyses; however, tools will never replace analysis and interpretation by humans, and increasingly, the availability of threat intelligence skills is falling short of demand.

Lessons Learned

In the discussions that followed each portion of the presentation, audience members shared the lessons they learned from the presentation and injected their own knowledge and experience into the conversation.

The audience identified the following key takeaways from the presentation:

1. Security is expensive, but insecurity is more expensive.

2. Cybersecurity is now a global issue with global players.

3. Available automated tools and processes make it easy enough to catch the unsophisticated criminals; determined, sophisticated actors do not make it easy.

4. Understanding the motivations of threat actors is vitally important: the who and the why.

5. In terms of innovation, the "bad guys" (criminal actors) are leading the industry. And, we should try to learn from them.

6. Anti-virus software gives users a false sense of security.

7. Big data analytics is growing in importance as we try to make sense of large volumes of data and detect patterns of interest, because individual malicious events or fraudulent behaviour may look similar or even identical to normal, everyday transactions.

8. The problem is acute in the banking industry, but it is not unique to it. However, the real issue stems from the software industry that underpins these other commercial industries.

9. Small and medium-sized businesses are particularly vulnerable and should practice ensure they have good Internet "hygiene".

10. There is a skillset shortage: we need more intelligence experts and data scientists.

11. Our current approaches are not working – there is a need for innovation, which will likely come through a paradigm shift.

12. The industry is too fragmented. There is a need for greater collaboration between governments, technologists, and industry: a holistic approach to security.

The Business of Cybersecurity

David Grau and Charles Kennedy

About the Speakers

David Grau is Vice President and Head of Threat Response, Intelligence, and Defensive Technologies at TD Bank Group. David has more than 20 years of professional information security experience and leads a multi-national team of information security specialists, with a global responsibility for providing TD Bank Group's Security Incident Response, Threat Intelligence, and Defensive Technologies programs.

Chuck Kennedy is the VP for Credit Card Technology for North American Credit Card for TD Bank Group. He is responsible for technology service delivery, project management, and technology innovation for the credit card businesses for TD. Chuck has been a member of the CIO Association of Canada and has served on the Canadian Banker's Association's (CBA), Canadian Financial Institution – Computer Incident Response Team (CFI-CIRT). Chuck holds the CRISC designation (Certified In Risk and Systems Control) and was educated in the United States, Europe, and Canada. He holds a BA in Political Science (Business minor) from the University of Calgary and an MSc in Information Technology (Information Assurance) from the University of Maryland – University College. His graduate work involved the study of geo-spatial intrusion detection and its integration with complex event processing.

This report was written by Chris McPhee

Citation: Grau, D. & Kennedy, C. 2014. TIM Lecture Series – The Business of Cybersecurity. *Technology Innovation Management Review*, 4(4): 53–57. http://timreview.ca/article/785

Keywords: cybersecurity, information security, banking, threats, targets, hacking, incident response, intelligence, analytics