Q&A

Chen Han and Rituja Dongre

Q. What motivates cyber-attackers?

A. The need to understand the motivations of cyber-attackers is great, given that "cybersecurity risks pose some of the most serious economic and national security challenges of the 21st Century" (The White House, 2009). However, the motivations behind cyber-attacks intended to cause economic impacts may be different from those posing a threat to national security. And, in many cases, the real purpose and primary objective of a cyber-attack may be hidden or obscured, even if the attacker claims responsibility (Shakarian et al., 2013).

Nonetheless, to help tease out and understand common motivations, cyber-attackers may be categorized, noting that a given attacker may belong to more than one category (Andress & Winterfeld, 2011). For example, politically motivated cyber-attacks may be carried out by members of extremist groups who use cyberspace to spread propaganda, attack websites, and steal money to fund their activities or to plan and coordinate physical-world crime (Gandhi et al., 2011). Generally, the reason for non-politically motivated attacks is generally financial, and most attacks are considered as cyber-crime (Andreasson, 2011), but many cyber-attacks are motivated by deeply-rooted socio-cultural issues (Gandhi et al., 2011).

As shown in Figure 1, cyber-attackers can be broadly considered "insiders" or "outsiders" (Russell & Gangemi, 1993), meaning that they act from within an organization or attempt to penetrate it from the outside.

The three basic categories of insiders are: i) disgruntled employees, who may launch retaliatory attacks or threaten the safety of internal systems; ii) financially motivated insiders, who may misuse company assets or manipulate the system for personal gain (although some insiders may be acting on ethical grounds or for other reasons); and unintentional insiders, who may unwittingly facilitate outside attacks, but are not strictly speaking primary attackers (Andress & Winterfeld, 2011).

Outsiders can be classified based on their organization, motives, and professional level: organized attackers, hackers, and amateurs.

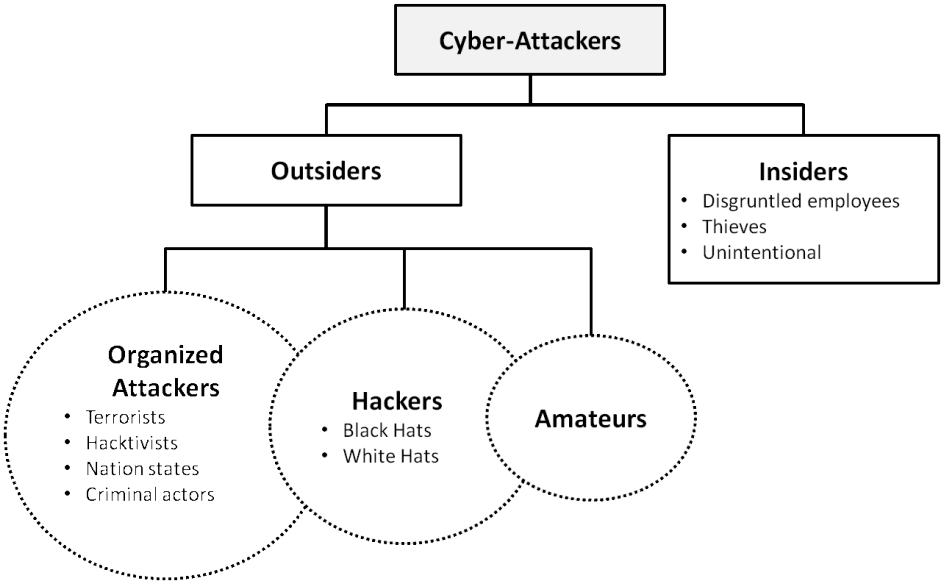

Figure 1. Categories of cyber-attackers

Q&A. What Motivates Cyber-Attackers?

Chen Han and Rituja Dongre

1. *Organized attackers:* include organizations of terrorists, hacktivists, nation states, and criminal actors. Terrorists are those who seek to make a political statement or attempt to inflict psychological and physical damage on their targets, in order to achieve their political gain or create fear in opponents or the public (Howard, 1997; Lewis, 2002; Cohen et al., 1998). Hacktivists seek to make a political statement, and damage may be involved, but the motivation is primarily to raise awareness, not encourage change through fear. Nation-state attackers gather information and commit sabotage on behalf of governments (Cohen et al., 1998), and are generally highly trained, highly funded, tightly organized, and are often backed by substantial scientific capabilities. In many cases, their highly sophisticated attacks are directed toward specific goals, but their specific motives may be mixed (Cohen et al., 1998). Criminal actors are usually "organized groups of professional criminals" (Cohen, et. al, 1998), and they may act within complex criminal ecosystems in cyberspace that are both "stratified and service oriented" (Grau & Kennedy, 2014). Perpetrators of organized crime are typically focused on control, power, and wealth (Gragido et al, 2012).

2. *Hackers:* may be perceived as benign explorers, malicious intruders, or computer trespassers (Hafner & Markoff, 1991; Lachow, 2009). This group includes individuals who break into computers primarily for the challenge and peer status attained from obtaining access (Howard, 1997). In some cases, hacking is not a malicious activity; a "white hat" hacker is someone who uncovers weaknesses in computer systems or networks in order to improve them, often with permission or as part of a contract with the owners. In contrast, "black hat" hacking refers to malicious exploitation of a target system for conducting illegal activities. In most cases, black hat hackers could be hired by or be sponsored by criminal organization or governments for financial gain or political purpose. Thus, hacking can involve espionage (i.e., to obtain secrets without the permission of the holder of the information, primarily for personal, political, or criminal purposes), extortion (i.e., to extract money, property, or other concessions by threatening harm), theft (i.e., to steal valuable data, information, intellectual property, etc.), vandalism (i.e., to cause damage) (Shakarian et. al, 2013; Cohen et. al, 1998; Howard, 1997).

3. *Amateurs:* less-skilled hackers, also known as "script kiddies" or "noobs" often use existing tools and instructions that can be found on the Internet. Their motivations vary: some may simply be curious or enjoy the challenge, others may be seeking to build up and demonstrate their skills to fulfill the entry criteria of a hacker group (Andress & Winterfeld, 2011). However benign their intentions may be, the tools used by amateurs can be very basic but powerful. Despite their lower skill skills, they can cause a lot of damage or, after gaining enough experience, may eventually "graduate" to professional hacking.

Although these categories are presented as discrete groups, there can be some overlap or difficulty placing a given situation into a particular box. For example, a group of hackers can act in a coordinated fashion, and in this sense could be considered "organized attackers."

The categories of cyber-attackers enable us to better understand the attackers' motivations and the actions they take. As shown in Figure 2, operational cybersecurity risks arise from three types of actions: i) inadvertent actions (generally by insiders) that are taken without malicious or harmful intent; ii) deliberate actions (by insiders or outsiders) that are taken intentionally and are meant to do harm; and iii) inaction (generally by insiders), such as a failure to act in a given situation, either because of a lack of appropriate skills, knowledge, guidance, or availability of the correct person to take action (Cebula & Young, 2010). Of primary concern here are deliberate actions, of which there are three categories of motivation (Gandhi et al., 2011):

1. *Political motivations:* examples include destroying, disrupting, or taking control of targets; espionage; and making political statements, protests, or retaliatory actions.

2. *Economic motivations:* examples include theft of intellectual property or other economically valuable assets (e.g., funds, credit card information); fraud; industrial espionage and sabotage; and blackmail.

3. *Socio-cultural motivations:* examples include attacks with philosophical, theological, political, and even humanitarian goals (Gradido et al., 2012). Socio-cultural motivations also include fun, curiosity, and a desire for publicity or ego gratification.

Q&A. What Motivates Cyber-Attackers?

Chen Han and Rituja Dongre

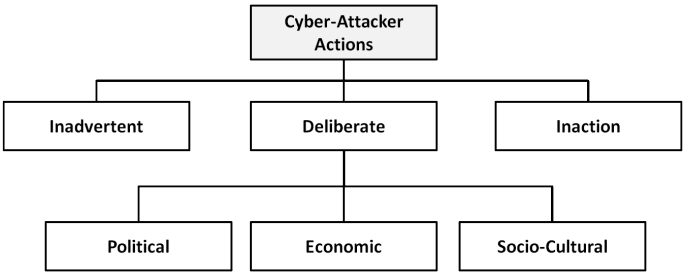

Figure 2. Types of cyber-attacker actions and their motivations when deliberate

About the Authors

Chen Han is a graduate student in the Technology Innovation Management (TIM) program at Carleton University in Ottawa, Canada. She has more than 8 years working experience in product design, User interface design and project management. She built and led an independent technical team that provides overall solutions and outsourcing services for various clients including world's top media, Internet startups, and multinational firms. Currently, she is working with founder team of Pricebeater, a global startup offering tools for online shopping in North America.

Rituja Dongre is a graduate student in Technology Innovation Management (TIM) program at Carleton University in Ottawa, Canada. She holds a Bachelor's Degree in Electronic and Telecommunication from the Nagpur University, India, and has worked as an Associate Consultant in Capgemini India.

Citation: Han, C., & Dongre, R. 2014. Q&A. What Motivates Cyber-Attackers? *Technology Innovation Management Review*, 4(10): 40–42.
http://timreview.ca/article/838

Keywords: motivation, cyber-attack, cybercrime, cybersecurity, hackers

References

Andreasson, K. J., 2011. Introduction. In K. J. Andreasson (Ed.), *Cybersecurity: Public Sector Threats and Responses:* XIII-XXV. Boca Raton, FL: CRC Press.

Andress, J., & Winterfeld, S., 2011. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Waltham, MA: Elsevier.

Cebula, J. J., & Young, L. R. 2010. *A Taxonomy of Operational Cyber Security Risks. Technical Note CEM/SEI-2010-TN-028.* Pittsburgh, PA: Software Engineering Institute.

Cohen, F., Phillips, C., Painton Swiler, L., Gaylor, T., Leary, P., Rupley, F., & Isler, R. 1998. A Cause and Effect Model of Attacks on Information Systems: Some Analysis Based on That Model, and The Application of That Model for Cyber Warfare in CID. *Computers & Security,* 17(3): 211-221.
http://dx.doi.org/10.1016/S0167-4048(98)80312-X

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. 2011. Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political. *IEEE Technology and Society Magazine,* 30(1): 28-38.
http://dx.doi.org/10.1109/MTS.2011.940293

Gragido, W., Molina, D., Pierce, J., & Selby, N. 2012. *Blackhatonomics: An Inside Look at the Economics of Cybercrime*. Waltham, MA: Elsevier.

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

Hafner, K., & Markoff, J. 1991. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York: Simon & Schuster.

Howard, J. D. 1997. *An Analysis of Security Incidents on the Internet 1989–1995.* Doctoral Thesis, Carnegie-Mellon University, Pittsburgh, PA.

Lachow, I. 2009. Cyber Terrorism: Menace or Myth? In F. D. Kramer, S. H., Starr, & L. K. Wentz (Eds.), *Cyberpower and National Security:* 434-467. Dulles, VA: Potomac Books.

Lewis, J. A. 2002. *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.* Washington, DC: Center for Strategic and International Studies.

Russell, D., & Gangemi, G. T. 1993. *Computer Security Basics.* Sebastopol, CA: O'Reilly & Associates.

Shakarian, P., Shakarian, J., & Ruef, A., 2013. *Introduction to Cyber-Warfare: A Multidisciplinary Approach*. Waltham, MA: Elsevier.

2009. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure.* Washington, DC: Executive Office of the President of the United States.
http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf