Arief, Budi, Bin Adzmi, Mohd Azeem and Gross, Thomas (2015) *Understanding Cybercrime from Its Stakeholders' Perspectives: Part 1 - Attackers.* IEEE Security & Privacy, 13 (1). pp. 71-76. ISSN 1540-7993.

Understanding Cybercrime from Its Stakeholders' Perspectives:

Part 1—Attackers

Budi Arief, Mohd Azeem Bin Adzmi, and Thomas Gross |
Newcastle University

Cybercrime is a term associated with activities relating to the misuse of data, computers, information systems, and cyberspace for economic, personal, or psychological gain. However, there's no authoritative definition or description of what cybercrime actually means, nor a comprehensive description of its traits.

To better understand the meaning of cybercrime, we propose the creation of a coherent model and taxonomy, starting with the stakeholders involved: attackers, defenders, and victims. Delving deeply into stakeholders' motives, cost models, tools, and techniques will provide a clearer picture of how humans interact with technology in the complex context of cybercrime. This improved understanding of cybercrime would contribute to better measures and awareness to prevent and combat cybercrime.

The Threat of Cybercrime

A July 2014 McAfee report states that the amount of global annual losses due to cybercrime is an estimated US$400 billion, with a conservative estimate of $375 billion and a potential maximum of $575 billion.[1] Although these figures could be seen as tremendously huge losses, the actual figures are hard to accurately pin down, even with the best intentions. Some argue that the cost of cybercrime is exaggerated and often biased. For example, Ross Anderson and his colleagues stated that these figures might be intentionally over-reported and that the cost of defending against cybercrime (by purchasing protection software or patching affected systems) is disproportionately bigger than the revenue generated by the perpetrators.[2]

Figures on cybercrime loss are usually based on data obtained through surveys, but survey science is difficult.[3] First, a representative sample of the population might not provide a representative sample of the losses. This is because losses tend to be extremely concentrated, with uneven distribution across the population. Second, cybercrime surveys are prone to be distorted by outliers. Even a single outlier—perhaps due to a lie, transcription mistake, or exaggeration—can lead to catastrophic error. Finally, cybercrime is affected by "surveying rare phenomena" risks. For example, a majority of those surveyed might not be affected, while those who are affected report figures at much higher or lower rates.

In addition, there's no authoritative source for calculating the exact amount of losses, and the amount cited is based on reported cases. Most cybercrime incidents go unreported, as many victims are reluctant to admit they were victimized or might not even realize they were attacked.[3] Although the exact number of losses caused by cybercrime is arguable, the fact that cybercrime is a rising threat is undeniable.

What Is Cybercrime?

Cybercrime is the combination of crime and cyberspace. Crime implies a behavior—performed by a perpetrator or an attacker—that is considered harmful and therefore has a potential cost to individuals or society.[4] In addition to monetary losses, cybercrime's effects can be physical (a building is demolished

1540-7993/15/$31.00 © 2015 IEEE

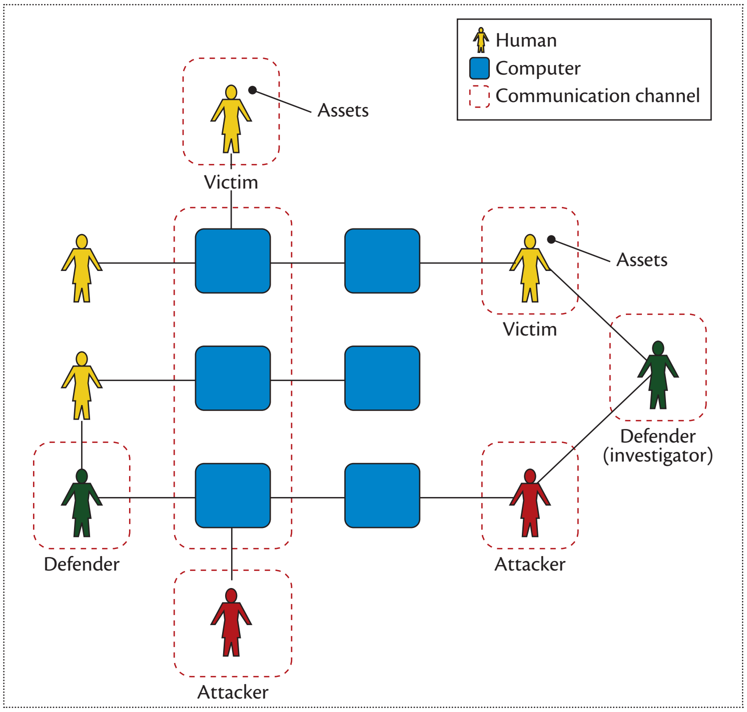

Figure 1. Cybercrime stakeholder interactions. A computer or network typically sits between an attacker and a victim, and—where applicable—a defender, representing the "cyber" element of cybercrime. Victims might have some assets that attackers are attracted to, but this isn't always the case. Defenders could be seen as entities associated with the entry point of an attack but might interact directly with victims and attackers in a noncyber environment (for example, a criminal investigator meeting with victims or arresting attackers).

or a person is injured), social (a person is shunned by society), or psychological (a person experiences depression, frustration, and anxiety). The crime might violate existing law (national or international agreements and charters) or might lie outside a clear jurisdiction (for example, international coercion cases with botnets).

The cyberspace component implies that there's always a cyber element, meaning that the crime is perpetrated over the Internet. Still, this classification isn't complete: cyberspace might be the medium for the crime, or it might be used by the perpetrator to gain more scalability. Graeme R. Newman describes cybercrime as a behavior in which "computers or networks are a tool, a target, or a place of criminal activity."[5] In addition, David S. Wall classifies cybercrime as crimes in the machine (computer content), crimes using machines (computer related), and crimes against the machine (computer integrity).[6] There's also the distinction of whether the crime is computer enabled (an extension of a traditional crime, made more scalable by technology) or computer dependent (the crime couldn't exist without technology).

Cybercrime might reach great scalability, meaning that it affects not only individuals but also groups and organizations, or even society as a whole. The crime might also be confined to a certain place or spread nationally or internationally.

Having a clear understanding of cybercrime from an individual to a societal level involves identifying and comprehending cybercrime stakeholders, who are classified according to their role in cybercrime incidents. These include attackers, defenders, and victims. Other stakeholders, such as middlemen or system operators, are beyond the scope of this article.

The attacker represents a crime's perpetrators; multiple attackers might act in collusion. The defender represents law enforcement agencies and security researchers who attempt to understand and prevent crime, develop protection mechanisms and countermeasures, and collect evidence or prepare for a court case. The victim (intended or otherwise) represents the target of cybercrime. Victims might or might not realize that they've been victimized, and the crime's impact varies considerably from embarrassment or financial loss to a national security breach or even loss of life. Figure 1 illustrates how cybercrime stakeholders might interact with each other.

Cybercrime Stakeholder: Attackers

Attackers are usually motivated by political or financial gain, or human factors such as revenge or curiosity. Attackers range from hobbyist and professional hackers to angry workers and jealous spouses to organized crime groups, political activists, or even spies.

There's a subtle difference between cyberattack and cyberexploitation.[7] Although both might employ similar techniques to penetrate their target's defenses, the outcomes differ. Cyberattacks aim to harm or damage the target, for example, by corrupting important data or causing a denial of service. Cyberexploitation, on the other hand, aims to extract information surreptitiously, as in cyberespionage. Nevertheless, the impact of cyberexploitation could be severe, ranging from economic losses, such as stolen trade secrets or business plans, to threats against national security, such as leaking military information. Both cyberexploitation and cyberattack can be carried out on the same target by the same perpetrator, but that's not always the case.

Attackers' behavior can be characterized by some objective (malicious or benign), intent (deliberate or accidental), and capability. More often than not, cybercrime incidents are considered malicious (and thereby deliberate), where the attacker has a motive and even a business model or strategy to capitalize on the crime.

To get a clearer picture of attackers, we must dig deeper into their characteristics, addressing the "what" (attacking threats, breach levels, and target objectives), "why" (objectives and motives), and "how" (attacking tools, vulnerability identification, and attacking methods).

Attacking Threats

We identified five factors related to attacking threats, or the kinds of activities—illegal or otherwise—that attackers might perform. The most widely noted attacking threat is computer intrusion, which is any malicious activity directed at a computer system or the services it provides, typically allowing an attacker some level of control of the target system. Examples of computer intrusion include hacking, bots, worms, viruses, spyware, and malware. Computer intrusion might also serve as a stepping stone for mounting other kinds of attacks and for covering the attacker's tracks. For instance, an attacker might take over a legitimate computer network and storage devices for distributing illegal materials, while keeping his or her own IP address hidden.

Another common attacking threat is online fraud, which is wrongful or criminal deception intended to result in financial or personal gain. Examples include financial fraud (email scams, phishing, and online credit card fraud) and identity theft. The term "online fraud" often encompasses both financial fraud and identity theft.

Copyright infringement occurs when someone other than the copyright holder uses a work without the owner's authorization. Examples include software piracy, illegal downloading of music or video without authorization, and copyright violation. This is often perceived as a minor threat, perhaps because the victim is often a big corporation or a wealthy celebrity. As such, it's frequently overlooked, and has even become acceptable to some. Moreover, not all copyright infringement claims turn out to be substantive in the end. The copyright holders might retract their claim due to the costs of pursuing a legal case, the difficulty in proving their case, or a change of heart. Nonetheless, copyright infringement is still a crime, and various organizations such as the Recording Industry Association of America are trying to address the problem by chasing the biggest offenders.

With the increased popularity of social media and social networking sites, the serious threats of cyberstalking and cyberbullying have emerged. Cyberbullying often starts with cyberstalking and escalates with a more focused attack directed at the intended victim. The popularity of online gaming and its social elements (for example, the ability to talk to or about your opponents in massive online role-playing games) has opened up a new type of cyberbullying, in which players harass and gang up on each other. The consequences of these attacks can be very harmful and even fatal, with reports of teenagers committing suicide after being bullied online.[8] A recent study by the Pew Research Internet Project indicates the prevalence of online harassment among US Internet users, with 40 percent of respondents having experienced online harassment (ranging from name-calling to being stalked), and 73 percent having witnessed others being subjected to it.[9]

Finally, there's the publication and sharing of illegal material online, such as inappropriate images of minors and items related to hate crimes and terrorist threats. The impact of these threats can be very tangible (for example, a person's life could be ruined or even ended) and wide reaching (a terrorist attack could maim and kill many innocent bystanders). However, cross-jurisdiction issues remain, as what is illegal in one country might be legal in others. For instance, it's against the law to sell Nazi memorabilia in France, but it's legal in the US. This is a complex matter that requires multiple perspectives to address.

Breach Levels

Breach levels relate to the extent of the impact caused by the attacker. This is associated closely with the CIA principle of security model: confidentiality (only authorized people are able to access the information), integrity (the information is accurate and can't be modified in an unauthorized manner), and availability (the information or service is available when needed).

An attack could breach the confidentiality of a victim's data, such as a person's bank details or a company's intellectual property. The original owner still has the data but could become a victim of financial or identity fraud or—as in cyberexploitation—might lose a competitive advantage. The breach could also affect national security.

On another level, the integrity of a victim's information could be compromised. In this case, the attacker tampers with the accuracy and representation of the original data by adding, modifying, or deleting pieces of information. For example, the attacker might alter someone's credit rating, which could lead to that person's inability to secure a financial loan.

The third breach level doesn't involve a victim's data directly, but rather its availability. In this case, an attacker prevents the authorized user from accessing his or her user account, data, or other information.

The most recent estimate of the average cost of a data breach to a company (based on the Ponemon Institute's research involving 10 countries) is $3.5 million, a 15 percent increase from 2013.[10] The same report also identifies three main causes of a data breach: malicious or criminal attack, system glitch, and human error. Malicious or criminal attacks involve negligent insiders—employees or contractors who inadvertently cause a data breach through carelessness—and malicious insiders, who intentionally cause the breach.

It's an unfortunate perception that many, if not most, data theft incidents were committed by trusted individuals who were given access to the information.[11] Employees or contractors could be influenced—through financial rewards or blackmail, or even as a result of an ideological change—to steal valuable information and pass it on to a third party.

In addition to financial loss and compromise of national security, other effects of data breach include damaged reputations and the loss of customer loyalty and trust. In the aftermath of such a breach, affected parties (typically the employer and affiliated individuals or organizations) must work to rebuild their brand and image.

Target Objectives

Target objectives straddle the "what" and "why" of cybercrime. An attacker's target could be categorized into the following main groups:

- personal accounts: computer login, email accounts, social networking accounts, and bank accounts, which could be exploited for direct attack, such as financial fraud, or as a stepping stone for a more elaborate attack, such as phishing;
- data: credit card details, bank account numbers, customer databases, transaction details, and private information such as email conversations, text messages, phone calls, and merger information and company account details, which attackers could sell to a third party;
- resources: system, computer, or network resources an attacker could use to commit illegal activities or to mount further attacks;
- component: taking control of computer, network, and mobile devices—often related to physical attacks in which the component provides an entry point for the attack (for example, disabling a car's alarm system before stealing it); and
- human factors: triggering the victim's emotions, such as anger, jealousy, or fear, or fulfilling the attacker's own emotional desires, including curiosity, revenge, or reputation.

Theft of intellectual property (IP) is a growing concern among organizations, especially in pharmaceutical drug manufacturing and the automotive and film industries. These industries have spent large amounts of money and resources in the research and development of their products, so it's understandable that they want to protect their competitive advantage. Meanwhile, rivals are keen to get their hands on certain IP to reap its benefits without having to spend the capital typically associated with such an endeavor. This could lead to illegal tactics such as espionage and theft. On the other hand, anti-copyright campaigners argue that robust protection of IP rights could lead to a monopoly by the IP holder, which might hamper creativity and progress.

Motives

In conjunction with the target objectives, there are many reasons behind attacks. An attacker might be financially motivated, either stealing money directly from the target or attempting to obtain valuable information about competitors, which could benefit the attacker directly or be sold to interested third parties.

In some cases, the attacker is motivated by political or reputational gain: he or she wants to obtain an advantage over a rival by gaining access to campaign plans or even carrying out a smear campaign.

Another motive is emotional gain. The attacker might want to feel some form of accomplishment, such as taking pride in being able to break into a secure system, or to exploit the victim's feelings through bullying.

Tools

From an attacker's viewpoint, a tool is an instrument for exploiting a computer or network's vulnerabilities. Simple attacking tools can include information exchange sites, user commands, or even physical access to the target device. The simplest tool is an information exchange portal, which allows potential attackers to share insights, techniques, and learning resources through published articles or Internet forums. However, some tools are very sophisticated, such as Trojan horse programs, computer viruses, or distributed tools (botnets).

Vulnerability scanners represent a suite of tools that could be used to identify a system's weaknesses before launching a full-blown attack against it. These tools are useful because they allow attackers to minimize wasted effort on hard-to-crack systems by first exploiting targets with obvious vulnerabilities. Examples include host discovery, port scanning, operating system detection, service discovery, authentication tools, and vulnerability assessment tools.

An attacker might also utilize specific hacking tools, which are mainly used to exploit the weaknesses detected by vulnerability scanners. The hacking tool is equipped with more powerful, often customizable features that let the attacker gain access to or control the target system. Examples of hacking tools include exploit kits, password crackers, rootkit tools, wireless hacking tools, and packet-crafting tools.

Attackers tend to use proxies to hide their electronic trails. By hopping through several intermediate proxies, such as compromised computers or networks, attackers make it difficult for investigators to trace the attack back to them. Anonymizing services such as Tor can also be used for this purpose. These proxies can speed up access to resources and multiply an attack's magnitude.

Vulnerability Identification

A system's vulnerability is a weakness that lets attackers gain entry to the system. *Design vulnerability* is inherent to the system's design or specification, where even a perfect implementation will result in a vulnerability or design flaw. For example, buffer overflow is an often-exploited design flaw.

On the other hand, *implementation vulnerability* is caused by an error in the software or hardware implementation of a satisfactory design. For example, the incompatibility of a platform makes it vulnerable to attack. *Configuration vulnerability* is the result of an error or oversight in the configuration stage, for example, using default passwords for system accounts, giving "world write" permission for new files, or enabling vulnerable services by default.

Attackers will try to identify these three generic classes of vulnerability, exploiting one or more of them to enter a system.

Methods

Attacking methods represent the manifestation of the attack and are often the first symptoms that alert defenders or victims to the attack.

Defensive mechanisms, such as intrusion detection systems, could detect early-stage attacking methods such as *probe and scan*, which attempt to gather information about a target to determine its characteristics, protection mechanisms, and vulnerabilities, which could lead to further attack. Other network monitoring tools deployed by the defender or victim could also detect flooding attempts, which are geared toward swamping the target with bad data to overload its capacity.

Most systems require user authentication before allowing access. An attacker might try to discover a legitimate user's authentication credentials to gain access, for example, by exploiting weak passwords or using brute force to guess or crack passwords. Social engineering, in which an attacker uses psychological manipulation (for example, pretending to be an authority figure or taking advantage of a victim's eagerness to please), could prove to be an effective technique for gaining access without technical skills or tools. Furthermore, an attacker might even try to bypass the authentication process by exploiting a system's vulnerability, such as a configuration vulnerability that leaves the password blank or a design vulnerability that causes buffer overflow and presents the console to the attacker. Another popular method involves *spoofing*: assuming the appearance of a different entity in network communications or services to persuade or trick the victim into revealing valuable information such as his or her password.

Once allowed entry, an attacker could perform *read method*, obtaining information from a storage device or other medium without making a copy of it; *copy method*, reproducing the information while leaving the original information unchanged; *modify method*, changing the contents or characteristics of a piece of information that could be detrimental to the owner; or even *delete method*, removing information or making the information irretrievable. All of these would affect victims to varying degrees, but often victims aren't aware of the breach until they're locked out of their own system or they notice some of their information is missing.

Figure 2 summarizes the characteristics of attackers, providing some insight into the "what," "why," and "how" of attacks.

The biggest challenge in understanding cybercrime relates to the massive landscape involved, making it impossible to encompass everything. So, it's important to limit the scope by providing a comprehensive view of cybercrime from a specific perspective (the stakeholder's point of view in this article) before attempting to construct the big picture.

Cybercrime poses an asymmetrical challenge. The potential return for cybercriminals is high, with relatively low risks. On the other hand, the cost of protecting cyberassets could be disproportionately large. For example, a cybercrime ecosystem defender will need to close all possible holes to minimize the risk of being attacked. Meanwhile, an attacker only needs to find one hole to exploit it. In addition, cybercrime literature tends to provide more detail from the attacker's viewpoint than from the defender's or victim's. For example, it's easier to find information on how attackers plan their exploit, the tools that were used, and the impact of the attack than it is to learn about defenders' efforts and assets. This perpetuates the stereotype that

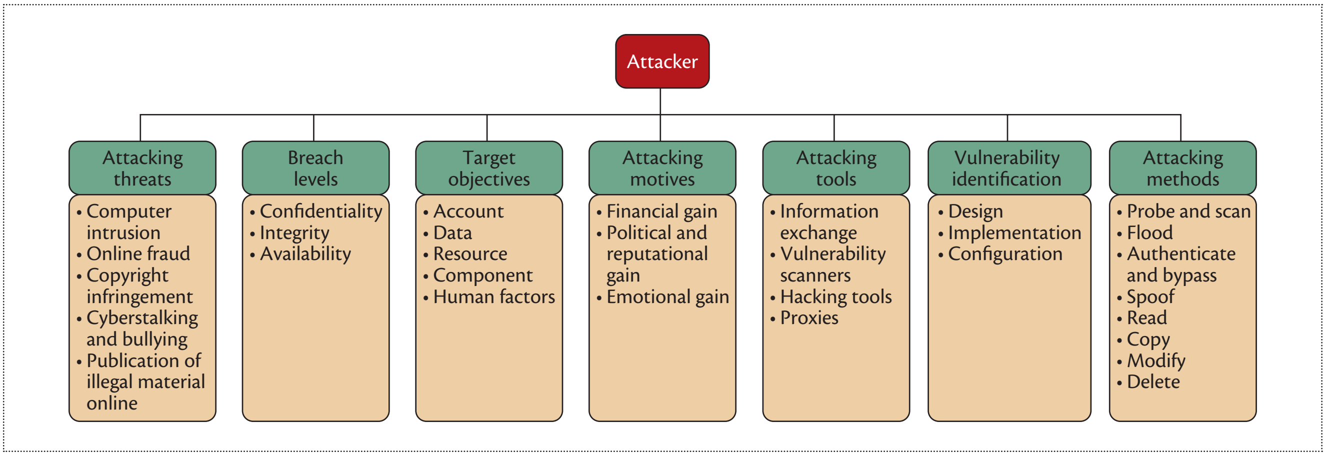

Figure 2. Attacker characteristics. There is a range of threats associated with attackers, who have reasons, tools, and techniques for conducting the attack. The potential damage caused by an attack varies in severity and targets.

attackers are smart people who exploit the limited skills or even the naivety of the defenders or victims. All of these aspects make it difficult to generate a balanced perspective on cybercrime.

The second part of this article, which will be published in the March/April issue of *IEEE Security & Privacy*, will analyze the victims' and defenders' roles in detail as well as lessons learned. We hope this series will provide an informative overview for understanding cybercrime, which in turn will raise cybercrime awareness and help combat cybercrime in a meaningful and practical manner. ■

References

1. "Net Losses: Estimating the Global Cost of Cybercrime," Center for Strategic and International Studies, McAfee, 2014; www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf.
2. R. Anderson et al., "Measuring the Cost of Cybercrime," *Workshop Economics of Information Security and Privacy* (WEIS 2012), 2012, pp. 265–300.
3. D. Florêncio and C. Herley, "Sex, Lies and Cyber-Crime Surveys," *Economics of Information Security and Privacy III*, 2013, pp. 35–53.
4. D.S. Wall, "The Internet as a Conduit for Criminal Activity," *Information Technology and the Criminal Justice System*, Sage Publications, 2005, pp. 77–98.
5. G. Newman, "Cybercrime," *Handbook on Crime and Deviance*, M.D. Krohn, A.J. Lizotte, and G.P. Hall, eds., Springer, 2009, pp. 551–584.
6. D.S. Wall, "Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace," *Int'l J. Police Practice and Research*, vol. 8, no. 2, 2007 (revised Feb. 2011), pp. 183–205.
7. "At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues," D. Clark, T. Berson, and H.S. Lin, eds., Committee on Developing a Cybersecurity Primer: Leveraging Two Decades of Nat'l Academies Work, Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences, Nat'l Research Council, National Academies Press, 2014.
8. C. Maag, "When the Bullies Turned Faceless," *New York Times*, 16 Dec. 2007; www.nytimes.com/2007/12/16/fashion/16meangirlshtml?pagewanted=all&_r=0.
9. M. Duggan, "Online Harassment," Pew Research Internet Project, 22 Oct. 2014; www.pewinternet.org/2014/10/22/online-harassment.
10. "2014 Cost of Data Breach Study: Global Analysis," Ponemon Inst., May 2014; www14.software.ibm.com/webapp/iwm/web/signup.do?source=gts-LITS-bus-conn-NA&S_PKG=ov23509.
11. "Privileged User Abuse & The Insider Threat," Ponemon Inst., May 2014; www.trustedcs.com/resources/whitepapers/Ponemon-RaytheonPrivilegedUserAbuseResearchReport.pdf.

Budi Arief is a senior research associate in the School of Computing Science at Newcastle University, England. Contact him at budi.arief@newcastle.ac.uk.

Mohd Azeem Bin Adzmi is a consultant focusing on IT strategy in Malaysia. He received an MSc in advanced computer science from the School of Computing Science at Newcastle University. Contact him at azeemadzmi@gmail.com.

Thomas Gross is an assistant professor in security, privacy, and trust at the School of Computing Science and the director of the Centre for Cybercrime and Computer Security at Newcastle University. Contact him at thomas.gross@newcastle.ac.uk.