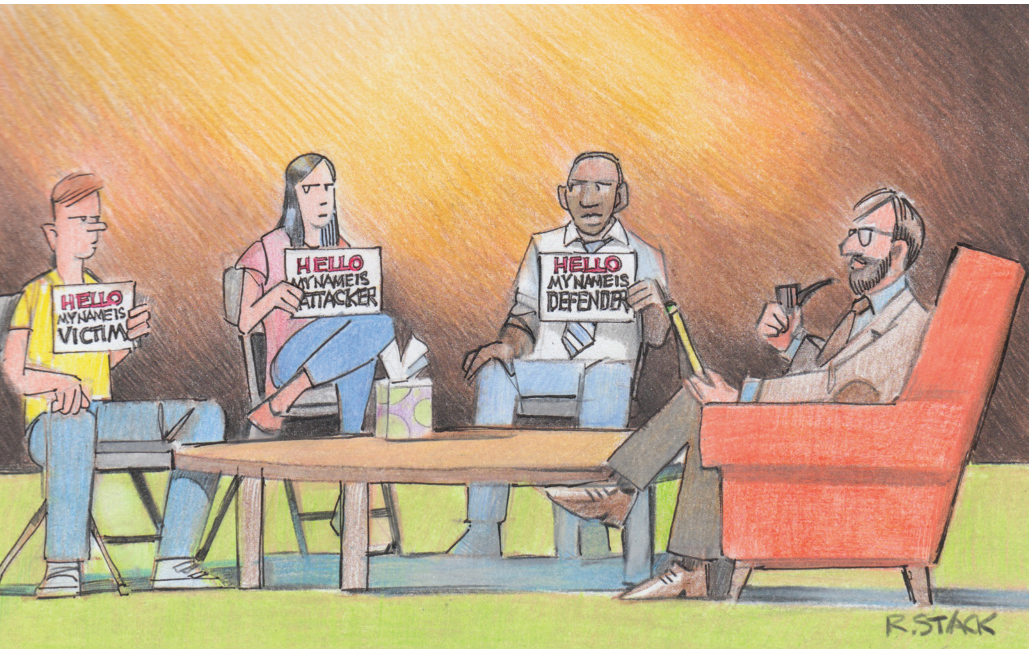
Editors: Richard Ford, rford@se.fit.edu | Deborah A. Frincke, debfrincke@gmail.com

Understanding Cybercrime from Its Stakeholders' Perspectives: Part 2—Defenders and Victims

Budi Arief and Mohd Azeem Bin Adzmi | Newcastle University



Cyberattacks are increasingly threatening the safety of cyberspace, as underscored by the recent attacks on Sony Pictures, Anthem, and Home Depot, to name just a few. Although the most tangible consequence of the Sony attack was the leak of confidential information, ranging from embarrassing email exchanges between Sony executives to copies of unreleased films,[1] it was more than just a data breach. Many stakeholders were affected, from the individual level to the organizational level and even the international level, with the resulting strain between the US and North Korea.

More worrisome—even though it hasn't been featured much in the media—is a recent cyberattack that caused physical damage to a steel mill in Germany.[2] This attack echoes the well-known Stuxnet incident.[3] In this case, the attacker manipulated and disrupted the mill's control system, which prevented a blast furnace from being properly shut down and caused unspecified damage. This incident raises further concern that the growing popularity of cyber-physical systems (especially in industrial control systems) could make society more vulnerable to cyberattacks.

As society grows more dependent on and intertwined with cyberspace, understanding and addressing various concerns regarding the human elements associated with cybercrime become more important.

Cybercrime Stakeholders

Cybercrime can be simply defined as activities relating to the misuse of data, computers, information systems, and cyberspace for economic, personal, or psychological gain.[4] However, cybercrime is much more complex than this definition suggests. For one thing, the accuracy of reported losses due to cybercrime is often arguable.[5,6] Because there's no authoritative body for reporting cybercrime, figures on losses are usually obtained from surveys, but mistakes and omissions are often made in data collection and analysis. Many other factors need to be considered, including the tools and methods used, cost and severity of the damage, attackers' motives, and impact to individuals and society.

Many stakeholders are involved with cybercrime. To allow for a meaningful discussion, we classify these stakeholders into three broad groups. *Attackers* are the crime's perpetrators, whose actions are considered harmful to other stakeholders and their systems and networks. *Defenders* aim to protect systems and prevent future attacks. In this article, we include investigators as a kind of defender. Investigators usually conduct an assessment after an attack and collect evidence to determine the cause of the attack and the extent of the damage. Investigators

1540-7993/15/$31.00 © 2015 IEEE

might take on the attacker role for undercover investigations, white hat penetration tests, and so on. Lastly, *victims* are the potential targets of cybercrime, whether intended or not. In many cases, stakeholders might play the roles of both defender and victim, especially if they're in charge of their own systems. Figure 1 shows how these stakeholders might interact.

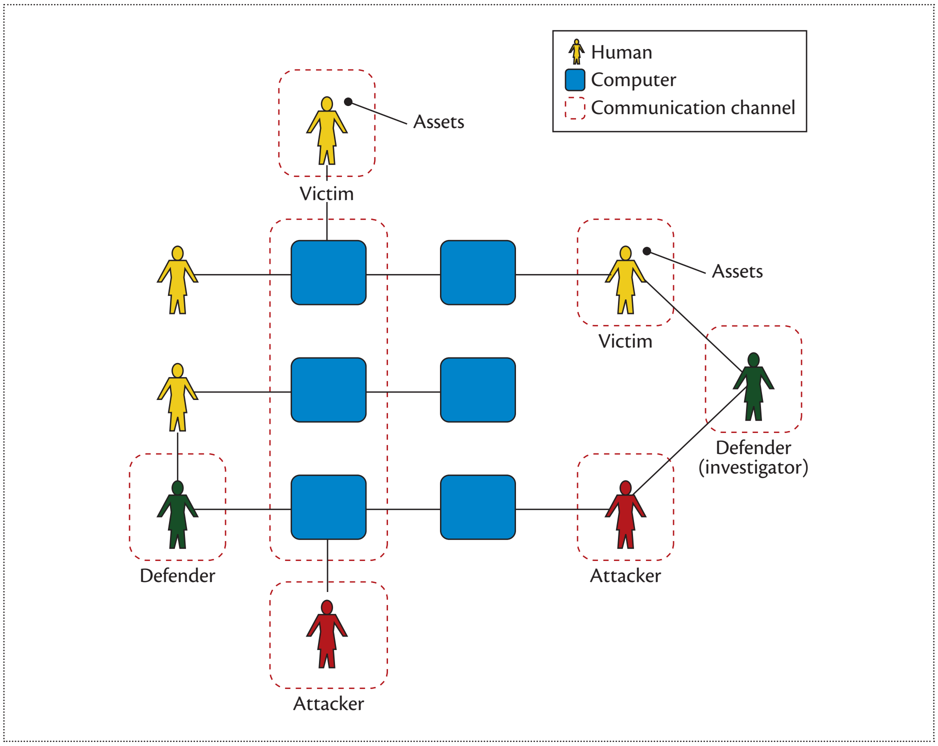


Figure 1. Cybercrime stakeholder interactions. A computer or network typically sits between attackers and victims and—where applicable—defenders, representing the "cyber" element of cybercrime. Victims might have some assets that attackers are attracted to, but this isn't always the case. Defenders could 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).

We discussed the attacker role at length in Part 1 of this article, which was published in the January/February 2015 issue of *IEEE Security & Privacy*.[4] To complete the discussion, we now look at the other two key stakeholders: defenders and victims.

Defenders

Defenders protect against cyberattacks that might be directed at them, their organization, or their clients and try to keep their assets or reputation from being impaired. Defenders could be considered an adversary of attackers: they're on opposite sides of the fence, and each side tries to prevent the other from achieving its goals.

As we did with attackers, we delve into defender characteristics by addressing the "what," "why," and "how." To avoid repeating ourselves, we highlight only a few key characteristics that need further discussion or are significantly different from attacker characteristics. Figure 2 shows a representation of defender characteristics.

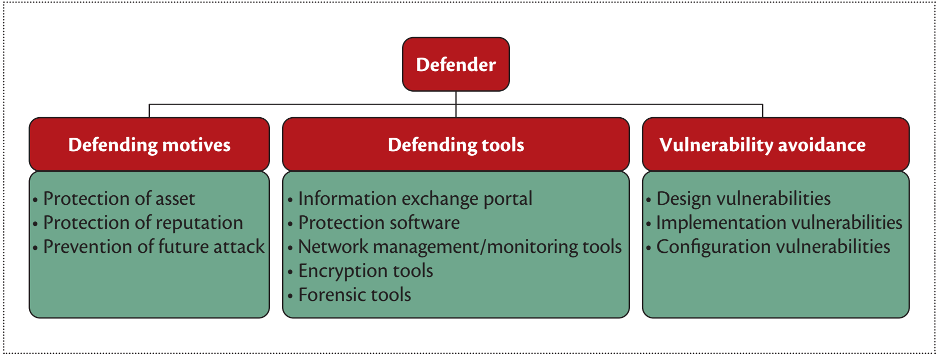

Defender
Defending motives
• Protection of asset
• Protection of reputation
• Prevention of future attack
Defending tools
• Information exchange portal
• Protection software
• Network management/monitoring tools
• Encryption tools
• Forensic tools
Vulnerability avoidance
• Design vulnerabilities
• Implementation vulnerabilities
• Configuration vulnerabilities

Figure 2. Defender characteristics. Defenders aim to prevent attackers from stealing resources or causing damage and, where possible, identify attackers and bring them to justice.

Defending Motives

Three main motives behind a defender's actions are

- asset protection—protecting accounts, processes, data, and other important information from unauthorized access;
- reputation protection—protecting more intangible properties such as societal status, market values, and consumer trust; and
- future attack prevention—finding ways to improve protection mechanisms and bring attackers to justice.

Asset and reputation protection play a big role in motivating defenders to prevent cybercrime incidents. The higher the stakes, the bigger the effort defenders need to make. Future attack prevention is relevant to the defender role as an investigator. By identifying and neutralizing the biggest offenders—such as the world's most prolific spammer[7]—we can expect a substantial reduction of the threat until the next generation of attackers emerges. The fight against cybercrime will continue to be a constant battle, and there will be enormous costs associated with defending and preventing cyberattacks—much bigger than the losses caused by the attack itself.[5]

Defending Tools

Defending tools are those that prevent computers or networks from being attacked, minimizing the damage or even fighting back.

Information exchange portals—such as online forums for sharing insights, techniques, and knowledge as well as more dedicated sites hosted by organizations such as the Computer Emergency Response Team Coordination Center—can help defenders find the information they need to respond to an attack. Other users might have experienced a similar attack in the past or might have compiled a list of countermeasures or remedial actions that could help defenders.

Protection software such as antivirus or malware removal kits can be used to detect, prevent, disarm, or remove malicious software. There are many vendors of such tools, and the quality of these products varies considerably, so it's important to choose products from reputable companies. Furthermore, some protection software claims to fix problems caused by viruses but actually install their own malware on the target system.

Many *network management and monitoring tools* let users observe and control incoming and outgoing network traffic. Their functions include but aren't limited to firewalls, intrusion detection systems (IDSs), packet sniffers, traffic monitors, getaways, and proxy servers. These can help defenders detect potential threats early and help investigators trace the source of an attack or build an attacker's profile.

To add an extra layer of protection, *encryption tools* and techniques can be used to prevent private data from being leaked through a security breach. At the very least, they can make it harder for attackers to get to the information.

Finally, *forensic tools* such as computer investigation and data recovery tools are of growing importance. These tools let investigators find evidence left by attackers.

Vulnerability Avoidance

Just as attackers have a propensity to identify existing vulnerabilities in a system, defenders also need to identify potential system vulnerabilities. Whereas attackers aim to exploit these vulnerabilities to commit a cybercrime, defenders endeavor to identify and patch these vulnerabilities before attackers can find them.

As we discussed in Part 1 of this article, three types of vulnerabilities must be considered. *Design vulnerabilities* are inherent in a system's design or specification; even a perfect system implementation will result in these vulnerabilities. Defenders use techniques such as formal methods to eliminate these vulnerabilities or techniques like fault tolerance to provide a graceful way to deal with such flaws. If system failure is unavoidable, the system will fail in a controlled manner so that damage or information leaks can be prevented or minimized.

Implementation vulnerabilities result from errors made in the software or hardware implementation of a design. Defenders can minimize implementation vulnerabilities using methods such as penetration testing, system testing, and a *hardening policy*—a checklist to help ensure that all computers are installed with the appropriate security measures.

Finally, *configuration vulnerabilities* result from system configuration errors. Defenders can protect against these using system validation and verification as well as penetration testing.

Victims

Victims are the targets of cybercrime attacks, intended or otherwise. Again, in many circumstances, victims are closely related to defenders. In an attack on an individual, the defender is likely to be the victim as well. In this sense, victims inherit many characteristics of defenders. However, as Figure 3 shows, three additional factors contribute to victims' characteristics: awareness and proficiency levels, attractiveness level and impact and cost to a victim.

Awareness and Proficiency Levels

Many cybercrime incidents occur because of victims' lack of awareness of security threats or low proficiency with regard to their ability to protect against these threats. Logically, those with very limited awareness of or knowledge about computer security often fall prey to attacks, whereas those with high knowledge and strong abilities might be able to resist or defend against attacks. However, very knowledgeable individuals or organizations can still become victims, often as a result of identity theft, insider threat, or cyberwarfare.

Attractiveness Level

Attractiveness level is mainly associated with a victim's assets, which can include finances, computing resources, or even a societal reputation. The more attractive the social profile or assets of an intended victim, the more attractive the victim becomes to attackers. Attractiveness level also relates to protection mechanisms. Attackers tend to go for easy targets first, especially if there's a smaller chance of detection. Wide-open networks or unpatched computers without firewalls or IDSs are examples of low-hanging fruit that attackers would exploit first.

Nonetheless, a victim's attractiveness is in the eye of the beholder.

It's not easy to determine why victims become targets as this depends on a range factors, including the value of victims to attackers, victims' ability to defend themselves, and the ease of the attack. Furthermore, some victims such as banks are attractive to many attackers, whereas others such as Sony Pictures have a very limited or niche set of potential attackers.

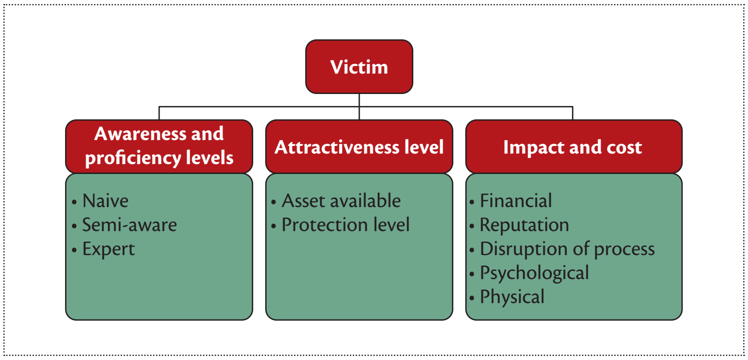


Figure 3. Victim characteristics. There are many different types of victims, ranging from individuals falling prey to Internet scams to nation-states being subjected to cyberattacks. The severity of the damage suffered by victims also varies considerably. This diagram provides a simplified view of victims' characteristics; further research needs to be performed to better understand victims.

Impact and Cost to Victim

The impact and cost to a victim tends to be proportionate to the victim's attractiveness level. These costs can be divided into five main categories:

- *financial*—money might be discreetly taken out of a victim's bank account or inadvertently transferred by a victim to an attacker through an online scam;
- *reputation*—a victim's reputation could be tarnished, leading to market value losses;
- *disruption of process*—online services or critical infrastructures could be disrupted;
- *psychological*—a victim can suffer from trust issues, anger, depression, or even fear for his or her safety; and
- *physical*—some attacks can cause physical harm, such as the nuclear centrifuges damaged by Stuxnet.

Lessons Learned and Recommendations

The best way to combat cybercrime is to understand it in detail, starting with the stakeholders involved. In many cases, preventive measures are relatively inexpensive and easy to implement. Users need to take steps to avoid becoming victims to cybercrime, and governments and industry need to be proactive in anticipating new threats.

We're still very inefficient at fighting cybercrime.[5] The costs of anticipating and preventing cybercrime, such as purchasing antivirus software and carrying out extensive penetration testing, are often much higher than the monetary losses caused by cybercrime. Furthermore, indirect costs, such as losses due to investigations and the interruption of service as well as psychological and emotional harm, tend to be disproportionately larger than direct costs. A more efficient approach in tackling cybercrime could include dealing directly with attackers by identifying and arresting them.

Emerging work in profiling potential victims could have a positive impact.[5] Being able to identify risk factors associated with a certain stakeholder—for example, an industrial control system operator—will enable a more effective set of detection, prevention, and protection measures for securing the stakeholder's assets or at least for mitigating and controlling the potential risk.

On an individual level, certain human traits—such as eagerness to please or willingness to trust others—make some people more susceptible to being a victim than others. There are many ways to profile potential victims: Olivier Thonnard and his colleagues used statistical techniques adapted from epidemiology to carry out a case control study that determines organizations' risk factors.[8] They found that the larger the organization, the more likely it is to be affected by a targeted spear-phishing email attack. It might seem intuitive to assume that some sectors like defense, critical infrastructure, or banking would be prime targets for an attack, but there are still many unknowns that need further substantiation. Understanding why and how some organizations or individuals are more likely to become victims is a complex issue.

The good news is that governments are beginning to pay more attention to cybercrime. For example, the Australian government developed its national plan to combat cybercrime in 2013. The plan outlines a framework in which the government will approach cybercrime using four key principles:[9]

- *Understanding the problem.* Identify the victims, how and why they were attacked, how the attack was carried out, who the perpetrators are, and how much harm was caused.
- *Partnerships and shared responsibility.* Tackling cybercrime is a shared responsibility among individuals, industry, and government.
- *Focusing on prevention.* It's better to prevent cybercrime from

happening than to respond to it after it's occurred.

- *Balancing security, freedom, and privacy.* Although it's important to uphold individuals' right to privacy, we also need to minimize the risk of security solutions being misused for cybercrime.

Armed with these principles, governments can shape policy and better allocate resources, and businesses and individuals can make informed decisions when assessing risks and taking protective action. Governments need to explore partnership arrangements, including with law enforcement agencies around the world; the education sector; and industry sectors such as Internet service providers, cloud services, e-banking, and online retail. Governments must take the lead on this matter, using their authority to highlight the importance of learning more about cybercrime to be able to prevent and defend against it effectively. Attackers must also understand and believe that they aren't untouchable and that they will be identified, arrested, and punished according to their crime.

Cybercrime is a worldwide issue. Various organizations, including governments, industry, research, and education institutions, will need to work together closely to construct a coherent strategy to combat cybercrime. This can be done through analyzing attack types, methods, and costs that span many sectors and multiple countries.

In the fight against cybercrime, teamwork is one of the keys to success. We need to implement proactive information and intelligence sharing among countries. We also need to develop a policy so that organizations can report cybercrime incidents to a regulatory body, which will result in precise statistics that can be shared across the globe. In certain countries, law enforcement's power to indict attackers isn't as strong as it could be, creating a gap in the prosecution of cybercrime offenders. For example, people who are indicted in one country might be able to hide in another country with a low enforcement level. It's crucial that governments take serious action to close this loophole.

Although it's projected that cyberthreats will continue to rise, raising cybercrime awareness will help combat this issue. Fighting cybercrime is an ongoing effort, and this article only scratches the surface. Further research on interdisciplinary perspectives of cybercrime is needed. We plan to delve deeper into policing cybercrime and its associated metrics, such as the cost of policing tasks and statistics of cybercrime in the public sector, as well as to explore other issues in human behavior and legal framework. Cybercrime can't be addressed with technical solutions alone, no matter how good security measures are. We also need to seriously consider the human factors that are involved. ■

References

1. "The Interview: A Guide to the Cyber Attack on Hollywood," BBC News, 29 Dec. 2014; www.bbc.co.uk/news/entertainment-arts-30512032.
2. K. Zetter, "A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever," *Wired*, 8 Jan. 2015; www.wired.com/2015/01/german-steel-mill-hack-destruction.
3. D. Kushner, "The Real Story of Stuxnet," *IEEE Spectrum*, 26 Feb. 2013; http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.
4. B. Arief, M.A. Bin Adzmi, and T. Gross, "Understanding Cybercrime from Its Stakeholders' Perspectives: Part 1—Attackers," *IEEE Security & Privacy*, vol. 13, no. 1, pp. 71–76.
5. R. Anderson et al., "Measuring the Cost of Cybercrime," *Proc. Workshop Economics of Information Security and Privacy* (WEIS 12), 2012, pp. 265–300.
6. D. Florencio and C. Herley, "Sex, Lies and Cyber-Crime Surveys," *Economics of Information Security and Privacy III*, Bruce Schneier, ed., Springer, 2013, pp. 35–53.
7. "Spammer Arrested and Charged with Fraud," *New York Times*, Jun. 2007; www.nytimes.com/2007/06/01/us/01spam.html.
8. O. Thonnard et al., "Are You at Risk? Profiling Organizations and Individuals Subject to Targeted Attacks," to be published in *Proc. 19th Int'l Conf. Financial Cryptography and Data Security*, 2015; http://fc15.ifca.ai/preproceedings/paper_57.pdf.
9. "National Plan to Combat Cybercrime," Attorney General's Dept. of Australia, 2013; www.ag.gov.au/CrimeAndCorruption/Cybercrime/Documents/National%20Plan%20to%20Combat%20Cybercrime.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. Contact him at azeemadzmi@gmail.com.

Got an idea for a future article?
Email editors Richard Ford (rford@se.fit.edu) and Deborah A. Frincke (debfrincke@gmail.com).