The Heritage Foundation

BACKGROUNDER
No. 3512 | JULY 24, 2020
CENTER FOR NATIONAL DEFENSE

Cybersecurity: National Policies and Practices for Understanding Hacks and Reducing Vulnerabilities

Klon Kitchen and James Di Pane

KEY TAKEAWAYS

Cybersecurity threats are real and tangible, with significant costs for governments, businesses and individuals, and they show no sign of receding.

Policymakers and other leaders do not need exhaustive cyber expertise, but they must know enough to make strategic risk and response decisions.

Cybersecurity is a posture that must be established and maintained, and both policymakers and individual citizens can take clear steps to adopt it.

One cannot mitigate a threat one does not understand. This is especially true in cybersecurity. Policymakers and other leaders do not need exhaustive cyber expertise; but they must know enough to make strategic risk-and-response decisions.

It is common for many information-security incidents to be called a "hack." But not all data losses are a result of someone engaging in "hacking" or of a system being "hacked." Instead, there are a host of cybersecurity threats that do not stem from hacks and are the result of other data-security vulnerabilities. Hacking is a real threat, however, that demands serious policymaker attention.

Hacking also does not simply happen. A hack starts with some kind of vulnerability, either technical or from bad cyber hygiene, which is then exploited by a bad actor. Reducing these

TEXT BOX 1

Brief Cybersecurity Guide

Three Core Aspects of Cybersecurity

1. Confidentiality: Limiting access to specific users
2. Integrity: Ensuring that the data is not manipulated
3. Availability: Ensuring that the network is accessible for authorized users

What Is a Hack?

- Unauthorized access to a computer network or data, not a data leak.
- Usually begins with a vulnerability that leads to a compromise.
- Vulnerabilities can be created through a wide range of ways like posting too much information on social media or clicking on links in suspicious emails, not just technical weaknesses in the system.

Two Primary Categories of Hacks

1. Computer Network Attacks: Breaking the system (Examples: Service Disruption or Ransomware)
2. Computer Network Exploitations: Stealing from the system (Examples: Intellectual Property Theft or Espionage)

Different Types of Hackers

- Insiders
- Criminals
- Hacktivists
- Terrorists
- Advanced persistent threats (APTs)
- State actors

Source: Ira Winkler and Araceli Treu Gomes, Advanced Persistent Security: A Cyberwarfare Approach to Implementing Adaptive Enterprise Detection, Protection and Reaction Strategies (Cambridge, MA: Syngress Publishing, 2017).

vulnerabilities would have a tangible effect on the frequency and severity of hacks. Improving supply-chain security, blocking attempts to create backdoors in software, and reducing vulnerabilities through use of good social media hygiene, password managers, and cybersecurity software can all help to reduce the number and severity of hacking attacks.

Context: Why This Matters

The effects of cyberattacks are real and tangible across a broad spectrum. They have significant costs for governments, businesses, and individuals. And, there is no sign of the threat of attacks receding. Cybercrime could cost the global economy $6 trillion in 2021 according to Cybersecurity Ventures.[1]

The five most attacked industries have remained consistent over the years: (1) health care, (2) manufacturing, (3) financial services, (4) government, and (5) transportation, not necessarily in that order. Ransomware attacks alone were predicted to cost the global economy $11.5 billion in 2019 and are currently projected to cost the global economy $20 billion in 2021, with an estimated ransomware attack every 11 seconds.[2]

The global COVID-19 crisis has increased the cyber threat further as more people telework and cyber criminals use click-bait to entice people to open corrupted files by couching them as information about the coronavirus. In fact, the Cybersecurity Infrastructure Security Agency (CISA) is warning that state-backed and criminal cyber actors are using the COVID-19 crisis as cover for a broad range of phishing and other attacks, resulting in as much as a 37 percent increase in attempted cyberattacks in April alone.[3]

What Is Cybersecurity?

Cybersecurity is about protecting computers, networks, and the data stored on them from malicious activity by unauthorized users. While the challenges of securing the intellectual property of a major defense contractor are different in degree from protecting the data on a personal smartphone, the premise is the same. It is about ensuring that only the right people have access, the data stays the way it was entered, and the legitimate users can access their system when they want to. Put another way, the three primary aspects of computer and network security are *confidentiality*, *integrity,* and *availability*.[4]

Confidentiality is about limiting network access to specific users in order to keep the data private. The network and the data stored on it should be limited to those who need to access it.[5] This is especially true when it comes to intellectual property, personal information, and other important information that people want to protect from outsiders. Medical records are a great example, as they are important to both the hospitals and the patients and contain a great deal of personal information. Maintaining confidentiality means that only health care providers and the individual patients see those records.

Integrity means protecting the data from being manipulated or tampered with by an unauthorized person. (This does not prevent data from being entered inaccurately or mishandled by an authorized user.)[6] A nurse or doctor mistakenly mislabeling a chart is sloppy data management. Someone changing medical records to create chaos for a hospital or to harm a patient is a security threat.

Availability means that authorized users have no trouble accessing the data they need. (While technical problems can and do occur, sometimes preventing legitimate data access, such problems require technical fixes to the network and computers themselves.) If an unauthorized person manipulates the network to prevent legitimate users from accessing their system or the data stored on it, that is a cyberattack. A hospital suffering from a ransomware attack that is unable to access its records without paying a large sum to a cyber-criminal would be an example of an attack on the availability of a system or data.

A compromise of any of these three aspects would result in damage to the network or the legitimate users of the network. Thus, cybersecurity is all about ensuring the confidentiality, integrity, and availability of a computer network and its data.

What Is a "Hack"?

A hack is "gaining unauthorized access to a system or the data stored on the system."[7] There are many ways this can be done, but at its core, it begins with a vulnerability in the system that allows a hacker access to information that should be secure. What is done with that access depends on the hacker and his or her motivation and technical competence. The two primary actions of hackers are computer network attacks and computer network exploitations.

There are many things that get mistaken for hacks or treated like the same thing. A data leak, for example, occurs when confidential data is exposed through poor network management. In that case, data that should be confidential can leak onto public networks or can be accessed by unauthorized people.

Issues with data can also be caused by user error or poor data hygiene practices during entry or management. These can create problems with real consequences, but they are not hacks or cybercrime. They are caused by the management of the data or network itself.

Attack or Exploitation? Important Differences

The main difference between a computer network attack and a computer network exploitation is that the first affects the functionality of the network,

while the latter compromises the confidentiality. One causes disruption and the other steals information.

Computer network attacks—cyberattacks—are "deliberate actions to alter, disrupt, deceive, degrade or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or network."[8] These cause damage or confusion and disrupt the regular functioning of an individual computer or entire network to achieve a desired end.

A computer network exploitation (CNE) is "the attack on the confidentiality of the targeted computer system. CNE is the theft of the data, with no other functions affected."[9] The goal of an exploitation is usually to steal data or gain intelligence on the compromised system for a future attack.

Four Types of Vulnerabilities Enable Hacking

Hacks begin when a bad actor finds a vulnerability in a network. The hacker exploits that vulnerability to gain access to the network and its data. While perfect defense is impossible and vulnerabilities are inevitable, many of them are easily avoidable with proper cyber hygiene and awareness. Non-cyber practices can also create cyber vulnerabilities, as people are often the weakest link in the cyber defense chain. There are four primary types of vulnerabilities that hackers can leverage to compromise a network: (1) operational, (2) personnel, (3) physical, and (4) technical.

1. Operational Vulnerabilities. Operational vulnerabilities basically arise from how data is stored, accessed, and used. They come from the practices used for handling data and access to data, and are one of the most common types of vulnerabilities that hackers exploit. In some cases, these can stem from poor governance, or lack of procedures for ensuring that technical security controls are well organized and maintained.[10] Poor security awareness among personnel, falling for phishing e-mails, for example, is another aspect of this type of vulnerability, and this lack of knowledge about threats or proper security procedures can create a weakness in the human factor of the system.[11] Re-using the same password for all bank, e-mail, and social media accounts is also an example of this.

Sensitive information posted on a company's website, or too much personal information posted to social media, can also create vulnerabilities by providing potential hackers with intelligence about an organization or individual they are looking to target. That security question about which middle school a person attended is most likely available on his social media account. This concept also flows into broader personnel vulnerabilities.

2. Personnel Vulnerabilities. Personnel vulnerabilities are linked to how organizations manage their employees—from hiring and training to maintaining them. Ensuring that job candidates are trustworthy, either through a background check or other process is only the first step in ensuring that the candidates do not become a security risk. Ensuring that they receive the proper security training is also a component. The broader piece to personnel security has to do with keeping employees motivated to not become security threats themselves. This gets at the heart of the insider threat. A disgruntled employee may seek to damage his or her organization, either through stealing from the company directly or enabling others to steal. The threat could also come in the form of them turning a blind eye to others' poor practices, stealing, or compromising networks. Organizations should be aware that disgruntled employees could be a cybersecurity risk, and should make the effort to reduce their number.[12]

3. Physical Vulnerabilities. Security guards who are not trained in what to look for, or who do not focus on potential security risks, can lead to a physical security issue, but often it is even simpler. Poor access controls and inadequate locking mechanisms can allow unauthorized access to sensitive areas of buildings, such as server rooms.

4. Technical Vulnerabilities. Technical vulnerabilities stem from weaknesses in the design, configuration, or maintenance of technology that allow unauthorized activity.[13] This is the type of vulnerability that can allow for a "zero-day" incident, a previously unknown vulnerability in software being immediately exploited. In some cases, hackers can continue to find vulnerabilities even after the software is updated and patched.[14] Zero Day hacks represent a relatively small percentage of hacks, but they are dangerous because they can compromise an otherwise secure network.

How a Hack Takes Place—the Cyber Kill Chain

Developed by Lockheed Martin, the Cyber Kill Chain provides a framework for thinking about the various stages of a hack.[15] The stages themselves are reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. Depending on the sophistication of the hacker or hacking organization, and the relative strength of the defender, some of these phases may be longer than others. For example, an advanced hacking group may spend months in the reconnaissance phase looking for a vulnerability, while a criminal may happen upon a vulnerability through a phishing e-mail that someone clicks.

Reconnaissance. Reconnaissance encompasses everything from selecting a target to identifying vulnerabilities. It involves target research, identification, and selection.[16] This is where the hacker identifies which computer, network, or data set is of interest, and begins collecting information to identify vulnerabilities. Since many organizations and individuals are not careful about what they post online, much information is often readily available. Social media, company websites, and other available information can be scoured to glean useful information. Advanced hackers often do extensive research on their targets, and are looking for something very specific.

Weaponization. The hacker then needs a payload (a piece of code) that will provide the desired access to the system.[17] Depending on the sophistication of the hacker, he will acquire this code by purchasing existing code online or writing his own.

Delivery. Once acquired or developed, the weaponized payload must be delivered to the target. The delivery stage is the actual transmission or infection of the weaponized payload to the targeted environment.[18] Phishing e-mails are common delivery mechanisms, as are payloads imported to networks using USB ports. Insider threats are also especially dangerous as delivery points due to employees' knowledge of, and access to, the system. Any network connected to the Internet is vulnerable to a hacker via the Web.

Exploitation. Exploitation is the "activation of the exploit payload."[19] The delivered malware activates within the targeted system. This is the beginning of the actual compromise.

Installation. Once the hacker has delivered and activated the payload, the malware is installed on the target. Installation of malware enables the hacker to access the victim's system remotely, and opens the door for continued access and control of the malware within the system.[20]

Command and Control (C2). Once the malware has been installed on the target, the hacker establishes the ability to communicate with and control the compromise. C2 is the "establishment of outbound communications from a victim system for secure communications between victim and adversary systems."[21] This is important in order for the hacker to be able to work within the system.

Actions on Objectives. The hacker now either conducts a computer network attack or computer network exploitation. This final phase is when the actual effects of the compromise occur; it is when the "adversaries accomplish target objectives,"[22] such as stealing data or disrupting the system and engaging in a ransomware attack.

Hackers: Spies, Criminals, and Terrorists

The main categories of hackers are insider threats, criminals, hacktivists, terrorists, advanced persistent threats (APTs), and state actors. However, the lines between them are often blurred, and hackers themselves will shift between them. This is part of the challenge of identifying these groups and their motivations. This spectrum represents everything from the individual amateur to the organized team of professionals, and all can compromise computer networks and the data stored on them.

Insider Threats. Insider threats stem from employees of an organization that abuse the credentials and access to a network, either by accessing data for which they are not authorized or by providing access to unauthorized users. The unique danger of an insider threat is that employees are well positioned to cause damage because they already have some permission for accessing the network, and may even have administrator access and intimate knowledge of the security measures, the data stored on the network, and possible vulnerabilities.

Criminals. A criminal hacker is an "unauthorized person attempting to compromise the security of a computer network for criminal purposes."[23] The sophistication of criminal hackers varies widely, but most are opportunistic and look for whatever vulnerabilities and information that present themselves. The more sophisticated the criminal, the more focused his search may be; he may share the modus operandi of advanced persistent threats, some of which are criminal enterprises linked to nation-states. These organized crime threats have vast resources, and the scope of their hacking is hundreds of millions of dollars.

Hacktivists. So-called hacktivists hack computers for political purposes.[24] A good example of a hacktivist organization is Anonymous, a decentralized group that has launched attacks on several governments, religious institutions, and corporations.[25] Like with criminal hackers, there is a wide variety of skill and resource levels among hacktivists, but the big difference is the goal and outcome. Whereas criminal hackers tend to seek quick monetary gain, hacktivists often seek the maximum damage for the targeted individual or organization.

Terrorists. Terrorist hackers use "fear, uncertainty and doubt to achieve a political goal."[26] Although they have not posed a significant threat to date, cyberattacks can create a great deal of fear and uncertainty, and thus the potential for terrorist activity is ever present.

Advanced Persistent Threats (APTs). APTs are essentially organized crime groups that sometimes work directly for state governments. For the

U.S., APTs are often associated with hostile countries, such as China, Russia, Iran, and North Korea.[27] They are very well organized and have advanced hacking capabilities. As the term implies, they also tend to be persistent against the targets they choose. They often specialize in a target set and work diligently to collect intelligence and find vulnerabilities. If the cybersecurity team can block an attempted compromise, they fight to maintain their access to the network. A good example is APT41, a China-affiliated hacking organization that conducts financially motivated cybercrime against a range of industries, while also acting in tandem with Chinese government objectives.[28] These two mission sets are often closely related, adding to the murkiness of discerning APT activity from the states with which they are affiliated.

State Actors. States are the most sophisticated cyber hackers given the resources at their disposal, including intelligence and military services. The four state actors that are the most active hackers are China, Russia, Iran, and North Korea. China has highly sophisticated cyber forces that target military and commercial intellectual property as a part of the regime's strategy to steal Western technology to bolster its economy. Russia also has advanced cyber capabilities that it uses to enact influence campaigns against the U.S. and other Western countries. Russia also carries out cyberattacks on critical infrastructure of countries in its region, such as the three Baltic states and Ukraine. Iran has sophisticated cyber tools that outweigh its geopolitical weight and are a part of its arsenal of asymmetric tools that include proxy terrorist organizations and cruise missiles.

Recommendations for U.S. Policymakers

Cybersecurity is not a one-time investment or act. It is a posture and a capacity that must be established and maintained. In order to move the United States closer to this posture, policymakers should:

- **Use all tools of national power to enhance cyber deterrence.** Cyber deterrence goes beyond cyberspace. Strengthening cyber defenses and retaliating in cyberspace are important aspects of deterrence, but there are many other ways the U.S. can exert pressure and impose costs on cyber adversaries. Some of these are: diplomatic action, cooperation reduction, visa restriction, financial sanctions, legal action, and military action. A consistent pattern of imposing meaningful costs for malicious cyber behavior will strengthen our cyber deterrence if applied consistently, and in some cases, publicly.

- **Make threat intelligence sharing a two-way street between the government and industry.** The U.S. government should be more proactive in sharing threat intelligence with industry, allowing better and more informed decisions to be made in the private sector. Over-classification of threat intelligence hinders industry's ability to prevent national security threats with its technology. Prudence should be used in deciding which information to share with industry, but threat intelligence should not be a one-way street of only industry sharing with the government. This type of intelligence can be shared without the risk of compromising sources and methods, as the threat and warning intelligence would just highlight practices and methods of adversaries. This would not compromise how that intelligence was collected, nor would it affect U.S. capabilities.

- **Minimize vulnerabilities by not allowing "backdoors" and enhancing supply-chain security.** Any foreign technology that creates vulnerabilities in critical infrastructure ("backdoors") to U.S. data should be blocked. Such a move will put significant pressure on China and others for their poor security practices, as well as incrementally improving the safety of hardware and software supply chains into the U.S. by increasing domestic security research. The U.S. should also encourage its Five Eyes partners—Australia, Canada, New Zealand, and the United Kingdom—to adopt a similar approach and practices.

- **Block investment from untrusted companies in key sectors of the American economy.** Foreign companies with a history of producing hardware or software with known vulnerabilities should be blocked from U.S. investments by the Committee on Foreign Investment in the United States. Such an effort would assist in managing the problem of Chinese investment in, or purchase of, American start-ups that are eager to obtain capital and willing to accept poor security practices to do so.

- **Encourage the private development of cybersecurity supply-chain ratings and accreditation.** Such a framework would contain different tiers or ratings for different levels of accreditation, ranging from minimal overview of a company's supply chain to in-depth analysis of specific products' supply-chain features. These different levels of accreditation will provide consumers with more information, with which they can make better, risk-based decisions.

Additionally, producers will find such accreditation valuable for selling their products, thus connecting security and a profit incentive. Instead of mandating cybersecurity solutions, the U.S. government should collaborate with the private sector. A specific way to encourage the adoption of this system would be to require government agencies that deal with large amounts of sensitive data, or have security-related duties, to purchase technology only from organizations that are accredited by this cyber-supply-chain ratings system. The Cybersecurity Maturity Model Certification (CMMC) established by the Department of Defense is a good example of such a program on the government side, and would require contractors to obtain certification on cybersecurity practices as part of acquiring contracts with the Defense Department.

Recommendations for U.S. Citizens

Individual citizens should adopt basic cyber hygiene practices to protect themselves and their fellow citizens from hacking and other cybersecurity threats. Americans should:

- **Move their information to the cloud and automate software updates.** Amazon, Google, Microsoft, and other cloud storage providers spend hundreds of millions of dollars every year to protect their users from cybercriminals. Americans should take advantage of their efforts by moving their most important information to cloud storage (and never forgetting to back up the information in the cloud). Microsoft, Apple, and others also have settings that will allow users to automatically apply software updates as they are released. Those who use devices provided by their employer should check with their IT departments about getting updates installed as soon as possible.

- **Use two-factor authentication (2FA).** 2FA is an additional layer of security that requires a user to provide not just username and password, but also another verification of identity before access is granted. This second verification can be the answer to a "secret question," a hardware token that verifies user identity, a smartphone, credit card number, or a fingerprint, face scan, or "voice print." Americans should enable 2FA on every device they have. 2FA can be cumbersome to set up, but not nearly as painful as recovering from identity theft or other cyberattack consequences.

- **Use a password manager.** Apps, such as 1Password, LastPass, and Zoho Vault, encrypt and store passwords, generate strong passwords, and allow the user access to all passwords across all devices. It is best to stay away from apps and password managers that do not use strong encryption, or that are developed by foreign companies—especially Russian and Chinese.

- **Clean up their online life.** Everyone should adjust their browser's security and privacy settings for increased protection. People must also remember to never open suspicious e-mails, download attachments from suspicious e-mails, or click links in suspicious e-mails. E-mails from unknown senders should not be opened. Banks and other service providers will not request sensitive information, such as birth dates and Social Security numbers, via e-mail—a clear tip-off.

- **Rely on professional antivirus products.** Computer owners should purchase an antivirus product that offers automatic updates. Bitdefender, F-Secure, and ESET all offer reliable products, as do many others. Like with password managers, it is best to buy American when purchasing virus protection.

Klon Kitchen is Director of the Center for Technology Policy, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation. **James Di Pane** is Research Associate in the Center for National Defense, of the Davis Institute.

Endnotes

1. Herjavec Group, "2019 Official Annual Cybercrime Report: Cybercriminal Activity Is One of the Biggest Challenges that Humanity Will Face in the Next Two Decades," 2019, https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf (accessed May 12, 2019).
2. Ibid.
3. Cybersecurity and Infrastructure Security Agency, "Alert (AA20-099A): COVID-19 Exploited by Malicious Cyber Actors," April 8, 2020, https://www.us-cert.gov/ncas/alerts/aa20-099a (accessed July 8, 2020), and Phil Muncaster, "Cyber-Attacks Up 37% Over Past Month as #COVID19 Bites," *Info Security Group*, https://www.infosecurity-magazine.com/news/cyberattacks-up-37-over-past-month/ (accessed May 12, 2020).
4. Ira Winkler and Araceli Treu Gomes, *Advanced Persistent Security: A Cyberwarfare Approach to Implementing Adaptive Enterprise Detection, Protection and Reaction Strategies* (Cambridge, MA: Syngress Publishing, 2017), p. 16.
5. Ibid.
6. Ibid.
7. Ibid., p. 41.
8. Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations* (New York: Oxford University Press, 2016), p. 174.
9. Winkler and Treu Gomes, *Advanced Persistent Security*, p. 18.
10. Ibid., p. 90.
11. Ibid., p. 91.
12. Ibid., pp. 96 and 97.
13. Ibid., p. 33.
14. Buchanan, *The Cybersecurity Dilemma*, pp. 172–174.
15. Lockheed Martin, "The Cyber Kill Chain," https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (accessed May 12, 2020).
16. Winkler and Treu Gomes, *Advanced Persistent Security*, p. 181.
17. Ibid., p. 182.
18. Ibid.
19. Ibid.
20. Ibid.
21. Ibid.
22. Ibid.
23. Ibid, p. 53.
24. Ibid, p. 56.
25. Lily Hay Newman, "Hacktivists Are on the Rise—But Less Effective than Ever," *Wired*, May 5, 2019, https://www.wired.com/story/hacktivism-sudan-ddos-protest/ (accessed May 12, 2020).
26. Winkler and Treu Gomes, *Advanced Persistent Security*, p. 65.
27. FireEye, "Advanced Persistent Threat Groups," https://www.fireeye.com/current-threats/apt-groups.html (accessed May 12, 2020).
28. Nalani Fraser et al., "APT 41: A Dual Espionage and Cyber Crime Operation," FireEye, August 7, 2019, https://www.fireeye.com/blog/threat-research/2019/08/apt41-dual-espionage-and-cyber-crime-operation.html (accessed May 12, 2020).