Reducing Cybersecurity Security Risk From and to Third Parties

A major lesson from the COVID-19 pandemic is that protecting oneself is only part of the solution that will put a stop to the virus. It is also important to prevent the virus from infecting others to mitigate disease cases, hospitalizations, deaths, and economic and social consequences.

When it comes to cybersecurity, the main objective to date has been protection, with much research and many products and services aimed at attempting to identify and stop cyberattackers in their tracks. Relatively little research has addressed how to stop malicious software (malware) that has already affected a system from infecting other systems within or external to infected organizations. Consider distributed denial-of-service (DDoS) attacks, wherein compromised systems (bots) may not seem to be adversely affected themselves but can become platforms for subsequent attacks on others. It is also worth investigating how to prevent indirect propagation of cyberattacks such as ransomware, where payment of ransoms by one entity encourages attackers to invade others.

The overall number and impact of cyberattacks can be reduced by protecting against malicious software so it cannot enter a system and spread to third parties, such as internal and external users, customers, suppliers and partners. A sufficient level of cybersecurity cannot be achieved unless and until both sides of the issue—protection and prevention—have been addressed. The incentive to protect oneself or one's organization is to minimize damage and related costs. The incentives to protect others are not as obvious, especially if the others are competitors or rivals. Achieving a global optimum will include the difficult task of requiring individuals to act in the interest of the group rather than the individual.

A Cooperative Approach

A leading cybersecurity expert, who was head of information security for a large financial institution at the time, once said in a closed meeting that he was only responsible for ensuring that cyberattacks specifically targeting his institution were not successful, and that, if the whole industry were to be under attack, he would not be held responsible if his organization also happened to be a victim. In

C. WARREN AXELROD | PH.D., CISM, CISSP

Is the research director for financial services with the US Cyber Consequences Unit. Previously, he was the business information security officer and chief privacy officer for U.S. Trust. He was a cofounder and board member of the Financial Services Information Sharing and Analysis Center (FS-ISAC) and represented the banking sector's cybersecurity interests in Washington DC, USA, during the Y2K date rollover. He testified before the US Congress on cybersecurity in 2001. Axelrod received ISACA's Michael P. Cangemi Best Book/Article Award in 2009 for his *ISACA® Journal* article "Accounting for Value and Uncertainty in Security Metrics." He was honored in 2007 with the Information Security Executive Luminary Leadership Award and received a *Computerworld* Premier 100 award in 2003. Warren's books include *Engineering Safe and Secure Software Systems and Outsourcing Information Security,* and he was the coordinating editor of *Enterprise Information Security and Privacy*. He has published more than 140 professional articles and chapters in books and has delivered more than 150 professional presentations. His current research activities include the behavioral aspects of cybersecurity risk management and the security and safety of cyberphysical systems, particularly as they relate to autonomous road vehicles.

© 2022 ISACA. All rights reserved. *www.isaca.org*

other words, he considered his job to be to protect his own organization, with little concern for preventing others from being attacked. This attitude is common in many areas of threat, including the pandemic and climate change. However, the result of such thinking is that everyone is likely to end up worse off (some more than others) than if a cooperative approach is used. Of course, there are exceptions, as some have profited mightily from the pandemic and from cybersecurity failures. Although there are institutions that facilitate the sharing of threat and cyberattack data among members, such as Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs),[1] in general, the cyberthreat landscape is a free-for-all in which the richer and stronger organizations tend to fare better. It will take the alignment of objectives and strong political will to create a cooperative environment where everyone (except cyberattackers) benefits to the greatest extent.

> "It will take the alignment of objectives and strong political will to create a cooperative environment where everyone (except cyberattackers) benefits to the greatest extent."

Encouraging desired actions requires some form of central control, leading to a so-called Pareto optimum, which is "an economic state where resources cannot be reallocated to make one individual better off without making at least one individual worse off."[2] This is the focus of behavioral economics, where individuals are encouraged or nudged—through the use of incentives and persuasion—to act in the best interests of the group.[3] But first, one must recognize that the current dominance of self-interest must be changed into an attitude of protecting one's own and other communities.

To achieve global optimization, there must be a controlling international organizational structure, generally accepted policies and standards, and implementable, effective incentives and disincentives. A proposed organizational structure and administration policies and procedures for cybersecurity are described in the article, "The Creation and Certification of Software Cybersecurity Standards."[4]

Intrusion/Extrusion and Infiltration/Exfiltration

For the most part, cyberattacks are deemed to be due to intrusions, and the result of such attacks is often the unauthorized release of data, which is termed "exfiltration." However, this usage implies that the damaging release of information assets is surreptitious. This is not always the case. Attackers frequently infiltrate organizations' networks and systems surreptitiously, but they may access information forcefully or claim it was accidental. These differences are significant because they suggest how systems and networks could be protected and how the release of data and software could be prevented.

For the purposes of this argument, intrusion, infiltration, extrusion and exfiltration are defined as:

- **Intrusion**—Hostile invasion of systems and networks by cyberattackers
- **Infiltration**—Surreptitious unauthorized entry into systems and networks using social engineering methods (e.g., spear phishing) to acquire legitimate credentials
- **Extrusion**—Unauthorized pushing of software, documents and data forcefully out of systems
- **Exfiltration**—Surreptitious, unauthorized extraction of software, documents and data from systems using regular means of communication by the organization such as emails and file transfers

Figure 1 shows methods for inserting malware or performing other nefarious actions and outputting sensitive information assets for various threats and exploits. The list is not complete, as the range of crimeware is continually expanding and changing, including hybrid attack methods such as evolved versions of ransomware.

However, the range of threats provides an overview of the following types of attack to which individuals, groups and organizations are subjected:

© 2022 ISACA. All rights reserved. www.isaca.org

FIGURE 1
Entries and Exits for Various Threats

Threat	Intrusion	Infiltration	Extrusion	Exfiltration
Virus/Worm	Initial infection by hacker and then infection from replicated malware	Not applicable	Transmission to other systems	May compromise systems and data leading to unauthorized release of sensitive data
DDoS	Not applicable	Use of stolen credentials to take over bots	Not applicable	Not applicable
Ransomware Espionage	Not applicable	Use of stolen credentials to take over internal systems and steal or encrypt data	Not applicable	May be combined with exfiltration of sensitive data and threats to release data to public unless ransom is paid
Internal Denial of Service (DoS)	Not applicable	Not applicable	Not applicable	May prevent intended distribution of data, email, documents and files
Malfunction	May be caused by damaging input, intentional or not	Not applicable	May release data as a result of malfunction	Not applicable
Failure	May be caused by damaging input, intentional or not	Not applicable	May release data as a result of failure	Not applicable

- Viruses and worms are malware programs that are opportunistic and gain entry when targets exhibit vulnerabilities. They do not usually target specific victims, but they can be made to do so.
- Denials of service are not dependent on finding vulnerabilities *per se* in the target organizations, unlike computer viruses, but they do seek vulnerabilities in bots to insert malware in them in preparation for launching attacks. When the hacker decides to attack, the bots are activated simultaneously and deluge the target with messages, overwhelming servers and causing them to shut down or crash. As a consequence, legitimate users are not able to access applications to conduct regular business.
- Ransomware and espionage attacks commonly follow the cyber kill chain (**figure 2**).[5] The sequence of phases (i.e., reconnaissance, weaponization, delivery, exploitation, installation, command and control, actions on objectives) derives from the military. Although the initial phases of the kill chain are the same for both ransomware and espionage, the former seeks payment to provide a key to decrypt the encrypted data, while the latter generally tries to remain unnoticed while exfiltrating sensitive personal data of customers and employees, intellectual property, and confidential emails.
- Internal denials of service usually result from errors by development or operations departments when, for example, installing new or modified software or incorrectly patching operational systems.

FIGURE 2
Phases of the Cyber Kill Chain

Phase	Name	Description
1	Reconnaissance	Harvesting information such as email addresses, conference information
2	Weaponization	Coupling exploit with a backdoor into deliverable payload
3	Delivery	Delivering a weaponized bundle to the victim e.g., via email, web, Universal Serial Bus (USB)
4	Exploitation	Exploiting a vulnerability to execute a code on victim's system
5	Installation	Installing malware on the asset
6	Command and Control (C2)	Command channel for remote manipulation of the victim
7	Actions on objectives	With "hands on keyboard" access, intruders accomplish their original goals

Source: Adapted from Lockheed Martin, "The Cyber Kill Chain," USA, 2011, *https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html*

© 2022 ISACA. All rights reserved. *www.isaca.org*

- Malfunctions and failures may be instigated by external players or may be due to errors by internal staff or suppliers.

System malfunctions and failure often result in the equivalent of internal denials of service, but they are usually unintended, unless caused by a malevolent insider. They are commonly the result of human error in the system development life cycle (e.g., from design, programming, inadequate testing), during operational changes (e.g., incorrect update application) or during regular operations (e.g., hardware component failure, loss of power).

From Threats Through Recovery

Figure 3 shows the likely motivation of a range of threats for both intentional and accidental attacks.

Viruses and worms are usually designed to inflict harm or damage to victims' systems. They are purposefully created and are subjected to development life cycles similar to those of legitimate systems, including a proof-of-concept phase where they may be tested against a small population of potential victims prior to full-blown release. This is termed "in the zoo". These tests can sometimes be detected, although they are mostly performed inconspicuously. When released in the wild, they replicate themselves across the Internet, infecting as many systems as they are able to before potential victims put up defenses in the form of antivirus products. The level of cleanup in the recovery phase is a matter of the degree to which systems were affected.

DDoS attacks are also intended to harm victims, but they are designed differently from viruses and worms in that the first step is to commandeer computers (bots) throughout the Internet, as with viruses, but the bots serve as stepping-stones. They are infected with software that is designed to generate many messages against specific targets. Upon notification by the central controlling system, the bots launch a tsunami of messages against the target, making it impossible for it to conduct business as usual. The remedies also differ. Third-party services offer the ability to absorb and screen a high volume of messages. Usually, the target organization will change its web addresses to avoid being swamped again.

FIGURE 3

The Sequence of Events and Situations for Various Intended and Unintended Threats

Intent	Threat	Motivators	Creation	Infection	Transmission	Response	Recovery
Yes	Virus/Worm	Cause harm	Proof of concept in the zoo	Release in the wild	Replication	Installation of antivirus software	Depends on impact
	DDoS	Cause harm	Proof of concept in the zoo	Compromise of army of bots	Triggering action	Use of DDoS service	Restore service
	Ransomware	• Gain money • Cause harm	Malware DoS	Gain access to systems and data	Encrypt sensitive data and exfiltrate	Pay ransom or reconstruct databases	Install better monitoring and detection
	Espionage	• Save money • Gain advantage	Phishing to gain access	Gain access to intellectual property	Trawl systems for secret data and documents	Remove unauthorized access	Improve identity and access management
No	Internal DoS	• Time pressure • Lack of knowledge	Damaging change or upgrade	Propagation	Unintended activation	Correct error	Introduce preventive measures
	Malfunction	Shortcuts	Inappropriate design or use	Deterioration of operation	Deterioration of operation	Correct units malfunctioning	Restore service
	Failure	Cost reduction	Inappropriate design or use	Deterioration of operation	Loss of operation	Repair and replace failed parts	Restore service and replace system

Ransomware and espionage are similar in that they both are designed to take over victims' systems. However, the motivation behind ransomware is to openly gain from direct payments, whereas the purpose of espionage is to obtain secret information that can be used at a later date to gain some form of advantage. In both cases, the initial goal is to gain access surreptitiously and investigate what is available. In the case of espionage, the attackers may benefit from insider information. The same could be true for ransomware, although there have not been any such disclosures in the press. Ransomware attackers become known to victims when they are ready to make their demands, whereas those involved in espionage aim to remain undiscovered as long as possible so that they can conduct their attacks on a continuous basis. Ransomware victims can either pay or try to recover their data from backups. There is little that espionage victims can do if they learn that they have been compromised; although, in some cases, they have sued attackers if they can prove that their information has been stolen.

It is important to differentiate between internal staff and insiders; the latter has a negative connotation, as it is often associated with insider threats. Internal staff, which includes employees, consultants and contractors, often require privileged access to do their jobs. However, such access can lead to and enable unintended errors or deliberate subversion. Those responsible for identity and access management—authentication and authorization—can make mistakes that deny access to valid users and customers or allow access to those who should not or should no longer have such access. The former actions might be considered internal DoS. Access may also be prevented for internal users and customers due to authorized changes to applications, systems or networks leading to nonavailability or unauthorized changes by miscreants.

Protection and Prevention

Information security professionals focus on protecting their own organizations' systems against cyberattacks with relatively little concern for others being attacked, that is, unless such attacks affect them directly, especially when suppliers and partners are attacked. Such third-party compromises can result in the organization bearing the digital or physical consequences or itself becoming compromised.

> "While it is helpful to request vendors, outsourcers and partners to commit to risk reduction in the contractual terms and conditions, it is even more beneficial for an organization to have direct access to partners' and suppliers' security monitoring systems."

There are a number of ways in which organizations may be able to obtain attack information from third parties, if they agree. Ideally, such requirements should be included in service agreements and partnership contracts for vendors, outsourcers, and partners, as listed in the article, "Using Contracts to Reduce Cybersecurity Risks."[6] Employment contracts, nondisclosure agreements and license agreements may also include requirements that protect organizations against third-party risk. While it is helpful to request vendors, outsourcers and partners to commit to risk reduction in the contractual terms and conditions, it is even more beneficial for an organization to have direct access to partners' and suppliers' security monitoring systems. In addition, there should be a requirement for a neutral organization to perform regular security audits for those third parties that have the potential of exposing the organization to the greatest risk.

ISACs and ISAOs are examples of communities that care about the prevention of other members being subjected to successful attacks, which is a consequence of such sharing of threat, exploit and event information. Furthermore, participating in these organizations reduces members' own risk.

Figure 4 illustrates the ideal circumstances in which organizations not only protect themselves, but also prevent malicious software from being transferred to others. Legitimate users, customers, suppliers, partners and others (e.g., law enforcement, regulators) are able to access and load information into an organization's systems in addition to those who have nefarious intentions, such as attackers and insiders. Attackers can include individual hackers, organized crime groups and nation-states. Insiders are distinct because they have authentic credentials and authorized access, which they use for nefarious purposes.

LOOKING FOR MORE?

- Read *Audit Oversight for Onboarding Vendors. www.isaca.org/audit-oversight-for-onboarding-vendors*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

© 2022 ISACA. All rights reserved. *www.isaca.org*

FIGURE 4

Incoming and Outgoing Data and Documents

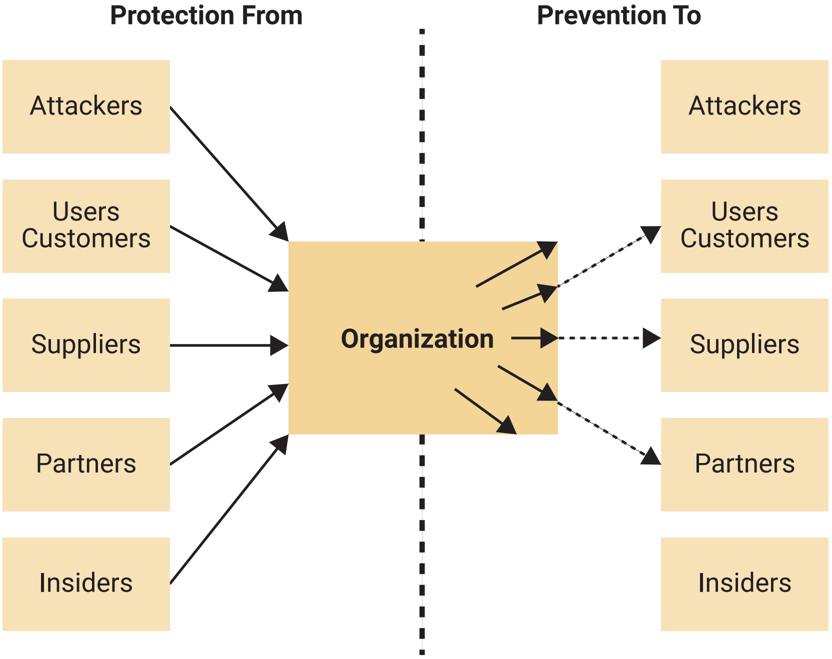

FIGURE 5

Protective and Preventive Measures

Protective Measures (Incoming)	Preventive Measures (Outgoing)
Antivirus software	Virus detection
Network, system and application firewalls	Not applicable
Honey pot	Not applicable
Intrusion detection system (IDS)	Detection of unauthorized exfiltration
Intrusion prevention system (IPS)	Prevention of unauthorized exfiltration
VPN	VPN
Content/source/destination monitoring	Content/source/destination monitoring
Behavior monitoring	Behavior monitoring
Air gap	Air gap
Physical media	Physical media
Obfuscation	Obfuscation
Tamper proofing	Encryption
Deception	Deception

These users reach the perimeter of the organization where the legitimacy of their messages is checked, and only those that are permitted under various criteria are allowed inside. In terms of output, the intention is to block unverifiable outputs at the perimeter and only allow approved messages (i.e., data, documents) to exit the organization.

As shown in **figure 5**, there are protective tools and mechanisms that attempt to protect the organization from attacks. Perhaps the earliest form of protection is antivirus software that detects viruses and worms and blocks their entry. The limitation of antivirus software is that it requires signatures of known viruses and does not protect from previously unknown malware. Other early forms of protection are firewalls—network, host and application—which determine the originating source of messages aimed at certain addresses and block those that are suspicious or otherwise unacceptable. The problem with firewalls is that there must be advance notice of what is deemed acceptable to enter (or not) so that intrusions can be blocked or guided into a honey pot, where the nature and intent of the malware can be examined without harm to the actual systems.

The use of encrypted conduits, such as virtual private networks (VPNs), helps secure the transmission of data. However, there is also a downside to encryption since nefarious encrypted messages cannot be examined.

More modern forms of protection monitor messages for origin and content and respond with information about unauthorized sources—as with IDSs—or preventive action—as with IPSs. Advancements in these systems include observation of unusual behavior and the use of artificial intelligence (AI) to determine threats.

A reliable means of protection is air-gapping systems so that there are no physical or wireless connections to the outside world. In such cases, data may be moved in and out of the system using physical devices, such as thumb drives. However, one should be aware that attackers have invented methods to circumvent air gaps through social engineering tricks (e.g., placing thumb drives containing malware in the parking lots of organizations with target systems hoping that an employee will pick one up and insert it into a computer connected to the internal system).

Other means of defense relate to confusing attackers and preventing them from carrying out their missions. Deceptive practices, such as honey pots, confuse attackers and make them think that they have broken into an unprotected system when, in reality, they themselves are being observed by defenders.

One might think that to prevent nefarious malware from being leaked, the same tools could be applied in reverse, that is, outgoing messages could be monitored with tools similar to the ones used to defend the gates. That may be the case, but, since there seems to be little incentive to make that effort, such a proposition has yet to be tested.

There are tools that monitor outgoing emails and files to ensure that they do not contain sensitive personal information or trade secrets, but those are for the benefit of the sender organization rather than the recipient, although the latter might benefit indirectly. Organizations often require that such sensitive information be encrypted; however, encrypted data cannot be monitored for the disclosure of information.

Preventing the Spread

How can the unauthorized release of sensitive data be prevented, especially when it causes organizations to incur additional costs and delays were they to implement the aforementioned measures?

It takes strong government intervention to encourage or force organizations to take preventive measures in the interest of all, even when such measures are not in the direct interest—or are even against the interests—of participants. When a model for such cooperation becomes available, then there is further incentive to develop the tools listed in **figure 5** if they have not already done so. The list of potential preventive measures is slightly shorter than that of protective measures, as shown in **figure 5**, because devices (e.g., honey pots, which comprise software to divert attackers to a designated safe area) are not appropriate for outgoing messages, although checking to make sure that one is not spreading a virus is a valid measure.

Conclusion

To make the Internet a more safe and secure environment for all, it is necessary not only to protect one's own systems, networks and data, but also those of other connected entities. Although the technologies to achieve this latter goal already exist to some extent in the form of message and file monitoring software, there is currently little incentive for organizations to take the initiative to prevent others from being attacked. It will be necessary to develop, implement, and enforce policies, laws and regulations that encourage or nudge organizations to act in ways that lead to global, rather than local, optima.

> "It takes strong government intervention to encourage or force organizations to take preventive measures in the interest of all, even when such measures are not in the direct interest…of participants."

Endnotes

1 The author was a cofounder of the Financial Services Information Sharing and Analysis Center (FS-ISAC), the first ISAC, launched in October 1999. The success of the FS-ISAC was largely due to a high level of interpersonal familiarity and trust among the government and private-sector participants—itself a rare achievement. Today there are dozens of ISACs and ISAOs, the latter catering to organizations that do not belong to a specific industry sector.

2 Investopedia, "Pareto Efficiency," *https://www.investopedia.com/terms/p/pareto-efficiency.asp*

3 Thaler, R.; C. R. Sunstein; *Nudge: Improving Decisions About Health, Wealth, and Happiness*, Penguin, USA, 2009

4 Axelrod, C. W.; "The Creation and Certification of Software Cybersecurity Standards," 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2016, *https://ieeexplore.ieee.org/document/7494112*

5 Lockheed Martin, "The Cyber Kill Chain," USA, 2011, *https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html*

6 Axelrod, C. W.; "Using Contracts to Reduce Cybersecurity Risks," *STSC CrossTalk: The Journal of Defense Software Engineering*, July/August 2017, p. 22–30.

© 2022 ISACA. All rights reserved. *www.isaca.org*