Is Cyberspace Secure From Humans?

A stable mechanism is one that operates consistently and sensibly. Cybersecurity is fundamentally a dynamic sociotechnical mechanism and, due to the human factor, it is vulnerable because human behavior and decision-making are complex and often unreliable.

Cyberspace is a wild frontier that has yet to be tamed. Cyberattacks continue to pose threats to data networks around the world. No amount of money, technology or hardware can provide complete protection from cyberattacks. Many believe that throwing technology at a challenge can solve it, but this is not always the case. The weak link in the cybersecurity chain is people.

Human Error in Cyberspace

The human factor is a major nontechnological stumbling block to cybersecurity. An organization's networks and data will not be secure unless employees obey clear, well-defined security policies and practice and participate in routine cybersecurity training and exercises.

According to an IBM assessment, human error is involved in 95 percent of information security errors.[1] Information management risk managers and chief information security officers (CISOs) should consider human fallibility, laziness and fatigue when creating and implementing policies and procedures to minimize security-related human error.

Human Fallibility

In some of the most successful attacks, threat actors exploit human laziness and fallibility. One survey showed that one in five enterprises (19 percent) that suffered a malicious data breach was infiltrated due to stolen or compromised credentials, increasing the average total cost of a breach for these enterprises by nearly US$1 million to US$4.77 million.[2] Organizations should work actively to remove the risk that comes from human laziness and fallibility, which, in turn, helps remove the threats that come with social engineering and phishing attacks. This can be helped by offering employee awareness training. Organizations should ensure all employees are familiar with the corporate security policy and are motivated to follow the rules.

Combating Laziness and Fatigue

Laziness can be the result of a lack of information. If communication is not clear or is nonexistent, then staff do not know what the organization's position is on security. The rules of the organization and why they exist must be clear and transparent; otherwise, it is easy for people to disregard them.

Gopikrishna Butaka, CISA, CDPSE, CEH
Is a manager of information systems audit at the State Bank of India (SBI), a Fortune 500 company with more than 22,000 branches worldwide. Apart from conducting various audits, which include IS audits, IT migration audits and regulatory framework implementation audits, Butaka's work also includes preparing and editing various policies for IT, cybersecurity and framework design. Butaka also coordinates the technical price negotiation committee, IT strategy committee and audit committee board meetings and ensures their implementation. Butaka is also an author focusing primarily on technology evolution and its impact on business and has contributed to dozens of articles for SBI's in-house magazines on technology and management issues.

> ON THE OTHER HAND, HUMANS CAN BE THE MOST EFFECTIVE SECURITY LINE FOR ORGANIZATIONS, SERVING AS EARLY WARNING SIGNALS OF CYBERESPIONAGE AND THREATS.

It should be a part of an organization's policy to give staff a checklist that includes all critical mandatory regular tasks and a self-enforcing metric to determine whether they have completed their tasks.

Although computers can work endlessly, humans are prone to fatigue when working longer hours, which makes them more prone to errors. Fatigue countermeasures include regulated working hours and mandatory breaks during work hours.

Lack of Strong Policies and Procedures

It is crucial to have strong policies and procedures in place on cybersecurity, data loss prevention (DLP) implementation, and IT and information systems procedures to protect the organization from various threats. As shown in **figure 1**, to help mitigate the risk of human error, security policies should clearly outline how to handle critical data and passwords, which security and monitoring software to be used, and who should access the software. Organizations should ensure that all the employees are familiar with the corporate security policy and are motivated to follow the rules. Organizations should allow privileged access only when needed on a case-by-case basis and monitor user activity to detect malicious activity. The lack of policies or gaps in implementation result in vulnerabilities. Periodic review of critical policies is also essential for effective implementation.

Defending Against Threats

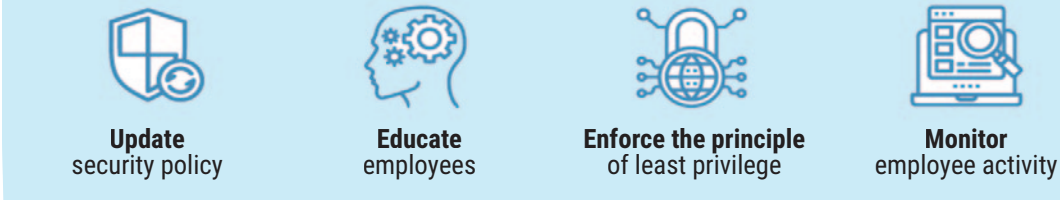
Governments and organizations are confronted with a hyperconnected environment in which wired networks jeopardize sensitive data and intellectual property. This sensitive information can be found in various places, including private and public clouds, removable media, and the handheld devices organizations use to do business. Because of the large number of computers in operation, protecting this data is challenging. Employees can use approximately 23,000 mobile devices in an average organization.[3]

When it comes to avoiding the exfiltration of mission-critical data, cyberdefenders face the most difficulties: a lack of visibility and background in how and where data are used as they spread through agency-issued, privately owned, and hosted applications and computers.

This environment provides adversaries with a rich area to target and exploit the data. Regardless of how attacks begin, they all lead to the same final intersections, where the most harm can be done. People come into contact with sensitive market data and intellectual property at these intersections, and the most comprehensively developed programs can be undermined by a single deliberate or unintended act at these human points of contact.

In 2020, the total average cost of insider-related incidents was US$11.45 million.[4] According to the Verizon *2020 Data Breach Investigations Report*, social attacks accounted for 22 percent of data breaches, and 8 percent of breaches were due to misuse by authorized users.[5] These threats are mostly based on finding human flaws in an enterprise's security protections.

Figure 1—How to Prevent Human Errors



Source: Ekran, "How to Prevent Human Error: Top 4 Employee Cybersecurity Mistakes," 24 September 2019, *https://www.ekransystem.com/en/blog/how-prevent-human-error-top-5-employee-cyber-security-mistakes*. Reprinted with permission.

On the other hand, humans can be the most effective security line for organizations, serving as early warning signals of cyberespionage and threats. A human-centric approach can be used to warn cyberdefenders, allowing them to avoid or deter sensitive data loss, regardless of whether the network has been compromised.

Security teams collect and sift through thousands of warnings (positive and negative) from the security operations center or monitoring system every day, and, as a result, they are losing the cyberwar. These security defenses can more rapidly detect cyberanomalies and gather the necessary context to distinguish between regular and disruptive or corrupted network activity warnings thanks to advances in human behavior and risk analytics. Integrated risk-adaptive and electronic compliance policies can then restrict or prohibit access to critical Internet Protocol (IP) based on the level of risk identified. Security teams gain the ability to understand, forecast and respond to possible attack incidents as they occur in this model, rather than weeks, months or years later.

Employees should be enlisted to help defend mission-essential and organizational properties. This improves defensive effectiveness within an organization and engages and consistently involves the organization's first line of defense—its people—in the security equation. To keep all people and data safe in a volatile world of hackers and industrial criminals, an "everyone-to-the-defense" joint project approach is essential.

> "FALSIFYING VIDEO AND AUDIO ARE COMMON PRACTICES USED TO DISTORT FACT AND PUBLIC OPINION FOR VARIOUS REASONS."

All organizations, large and small, want robust and efficient strategies for safeguarding sensitive information, such as trade secrets and digital crown jewels. The solution may be as simple as having a strategy that combines the human aspect with technology control.

Automating Cyberspace

Process automation eliminates the often-unreliable human component, resulting in more effective and consistent IT operations. Whether it is automating reports, updating software, checking the workstations and servers for changes, or doing routine maintenance, automating the IT infrastructure or using integrated systems management solutions saves time and eliminates danger.

IT process automation tackles human errors in the following ways:

- **Performs repetitive tasks**—Workers who do routine activities are more likely to get bored, and bored employees are more likely to make mistakes. Automation can perform the repetitive tasks that staff often complete, leading to a decrease in staff errors. General computer maintenance often strips IT administrators of large amounts of time. Creating an automatic script to complete general maintenance avoids the loss of time taken to do it manually and eliminates human error in IT.
- **Installs security updates**—Security patches and fixes must be regularly implemented in systems, including in servers, workstations and, most important, software. Organizations can create an automatic mechanism to search for and deploy pending upgrades using software, ensuring that their environment's components are kept up to date without the need for human interference. This not only speeds up the security patching operation, but also eliminates IT human error.
- **Automates monitoring**—IT administrators often fail to configure monitoring after a new server is set up because it is a daunting and time-consuming task. Automated monitoring scripts means that monitoring is installed as soon as new servers are added to the environment. This reduces human error and eliminates the possibility of failing to configure surveillance after the server goes down.

Automation not only minimizes human error, but it also saves time and resources. Using an IT automation framework for the small tasks that take up a lot of time frees system managers to work on more complex tasks and lowers the risk of human error in IT.

Enjoying this article?

- Read *Implementing Robotic Process Automation. https://www.isaca.org/rpa-survey-2020*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Deepfakes and Cyberattacks
Cyberattacks are nothing new. Organizations are already mindful of the vulnerabilities to industrial Internet of Things (IoT) networks' cybersecurity and have implemented solutions to mitigate the risk. Deepfake identification technology, on the other hand, is only in its infancy. Deepfake technology is expected to be a significant hazard in 2021, potentially resulting in substantial financial losses in a global economy already rocked by COVID-19. Falsifying video and audio are common practices used to distort fact and public opinion for various reasons, including slander, misinformation and psychological terrorism.

Several instances have been identified of cybercriminals impersonating chief executive officers (CEOs) and requesting the illicit transfer of corporate funds using artificial intelligence (AI)-based deepfake technologies.

Several technologies can be used to detect fake video and audio. Still, organizations can take some security steps to discourage the manipulation of their confidential data. AI-based technology to combat deepfakes includes adding noise pixels to images to avoid alteration, such as testing frames or the acoustic spectrum to find any distortions. Furthermore, an adequate employee preparation policy on managing classified or confidential business details should be implemented.

> "IT IS CRITICAL THAT STAFF ARE HELD ACCOUNTABLE FOR CYBERDEFENSE."

Cyberspace Security Measures

For several years, psychologists and other behaviorists have experimented with the idea of using a "nudge" to change a variety of behaviors. In terms of cybersecurity, a behavioral nudge is a technique to ensure that business insiders are mindful of the dangers of inaction regarding the very concrete threat of cyberbreaches. Using these ideas to teach cybersecurity could help people become more proactive. It is critical that staff are held accountable for cyberdefense. Increasing user understanding of the importance of data security, particularly in light of regulatory requirements such as the EU General Data Protection Regulation (GDPR), is a positive development.

According to one report, human error accounted for 24 percent of cybersecurity attacks in 2019, second only to phishing/malware at 31 percent (which still requires human error to activate).[6] Password sharing, patch management issues, double-clicking on insecure URLs and corporate access from mobile computers are only a few examples of human mistakes that can result in security breaches, all of which can be avoided.

Social Engineering Awareness
By using social innovation, anyone can hack into a system in a variety of ways, for example:

- Spear phishing emails are typically sent to a limited number of possible victims in an attempt to trick the recipient.
- A hacker attacks an organization's network and then claims to have discovered the breach's cause and offers to assist in fixing it. If the hacker's assistance is acknowledged, they can gain access to the device.
- An intruder may attempt to access a user's account and scan their communications for PDFs, video files and other types of downloadable material. A malicious code will then be inserted into another script, perhaps labelled as an updated edition, and submitted to the unwitting victim to open.

To avoid social-engineering threats, organizations can implement the following processes:

- Organizations should educate employees to not click on links, download files or open email attachments from unknown senders.
- Organization should use anti-phishing features offered by their email client and web browser.
- Organizations should secure all the devices used and install, maintain and regularly update their antivirus software, firewalls and email filters.

- Organizations should monitor URLs of websites used by employees on the network and look for a closed padlock icon—a sign the employee or organization's information will be encrypted.
- Organizations should set up and enforce multifactor authentication (MFA).
- Employees should be tested by having an outside party conduct periodic social-engineering tests.

Vendor Security
It is critical for organizations to know how safe outside vendors they partner with are. In 2020, General Electric suffered a breach from what most would consider a mundane, low-risk vendor, the human resources document management vendor Canon Business Process Services. The breach included the personal information of more than 200,000 current and former employees.[7]

Organizations should inquire about the surveillance mechanisms and tracking tools their vendors use. They can also request copies of their vendors' IT technology audits to ensure that adequate protections are in place. Finally, organizations should strongly advise vendors to use shift-detecting tools to detect whether any of their processes have been altered.

Change Detection Software
CimTrak, for example, is a robust encryption, reputation and enforcement framework that can be distributed and scaled to the largest global networks.[8] This automated software detects processes and provides versatile solution options and auditing capability, making it an effective cybersecurity platform. This kind of application can also assist organizations in determining:

- Who made a change to the data
- What changes were made
- Where the changes reside
- When the changes took place
- How the change was implemented

CimTrak's self-healing program can be used to restore unwelcome modifications to their original state without any downtime.

> "ALL REMOTE ACCESS SHOULD ROUTE THROUGH A PRIVILEGED IDENTITY MANAGEMENT SOLUTION (PIMS) AND BE LOGGED."

Periodic Audits and Analysis
Periodic cybersecurity audits of critical areas, meaningful analysis of the audit reports and implementing solutions to bridge the gaps help build a strong cybersecurity culture in an organization.

Best Practices for Combating Human Error

There are several best practices that help minimize the risk of human error and automation, including these:

- Organizations should dedicate at least 5 percent of their annual IT budget to defense to ensure that they have the necessary equipment, because effective security is less expensive than the cost of a data breach.
- Organizations should conduct periodic planning of information security and stick to the plan:
  - **Immediate term (0–3 months)**—Organizations must secure remote access and collaboration services, increase antiphishing efforts and strengthen business continuity. Organizations should manage access and monitor activity on all critical assets.
  - **Near term (3–6 months)**—Securing end users and data are the next priorities. Budget rebalancing may be needed as other projects are put on hold to safeguard the organization and invest more in security-related works.
  - **Medium to long term (12 months)**—Organizations should invest in zero trust, software-defined security, secure access service edge (SASE) and identity and access management (IAM), and automation to improve the security of remote users, devices and data.
- Organizations should invest time in training their employees and hold information security sessions periodically to assess employee knowledge of passwords, firewalls, ransomware, add-ons,

> "ORGANIZATIONS THAT HAVE ALREADY LEARNED FROM STABLE REMOTE WORKING CAPABILITIES ARE WELL ABLE TO DEAL WITH THE ONGOING RISE OF CYBERATTACKS."

Universal Serial Bus (USB) keys and other external memory discs; discuss current risk scenarios; and explore best practices and procedures.

- Organizations should ensure that all critical areas have implemented digital forensics and periodic assessment of the digital forensic readiness is carried out.
- All key stakeholders should be educated about the protection of personally identifiable information (PII) data and financial data and made aware of how to prevent phishing attacks.
- All remote access should route through a privileged identity management solution (PIMS) and be logged.
- Organizations should ensure that the activity data from firewalls, intrusion detection systems (IDS) (network and host) and the application log from the cloud management console are sent to the security information and event management (SIEM) team for analysis, along with the access monitoring data.
- Organizations should control, track and upgrade who has access to what data and ensure that each employee has their own unique password that they do not share with anyone else.
- Organizations should set up a multifactor security policy and a strict password policy for all applications.
- In relation to endpoint security, each employee's computer should be secured, and antivirus and antimalware programs should be authorized, installed and upgraded as needed.
- Organizations should use virtual private networks (VPNs) to ensure that the link is safe, encrypted and shielded both inside and outside the workplace.

The Digitalization Push of the COVID-19 Pandemic

As organizations adapt to new operating models based on the COVID-19 pandemic in which working from home has become the new normal, new challenges have emerged. Organizations are speeding up their digital transformation and cybersecurity efforts and are working to switch their working system to more technology-based platforms, such as cloud data sets and IoT. This does not mean simply implementing VPNs. Organizations have recognized that applications that promote productivity, collaboration and positive end-user experiences are a priority for creating a healthy remote workforce. To restrict the spread of breaches, limit entry and discourage lateral migration, organizations are following a zero trust mentality in which they follow the philosophy of "never trust, always check." There is no guarantee that anything employees do will be safe. This pandemic has shown that the secret to effectively limiting the threats associated with cyberattacks is to plan ahead. The ability to respond rapidly to unexpected incidents helps mitigate the effects of a cyberattack. Organizations that have already learned from stable remote working capabilities are well able to deal with the ongoing rise of cyberattacks, but those that were caught off guard need to determine their cybervulnerability risk quickly and prioritize measures to close cybersecurity holes in accordance with best practices. Furthermore, with organizations allowing remote access to classified and sensitive data, enterprise-owned computers should be the norm.

Conclusion

Any human error in the workplace can have a cascading impact on an organization's facilities, operations, client relationships and credibility. As a result, having robust polices and processes in place to reduce human error is critical. Users must take precautions to defend themselves and the data for which they are responsible. Organizations and employees must be vigilant and not let naivety, laziness or dissatisfaction with the work environment come to the fore. The most cutting-edge technological tools for network security can be created and implemented, but they are

ineffective if they are not adequately implemented, configured and managed. Worse, they can often provide a false sense of security. Information systems, cybersecurity and IT policies should be designed with all aspects of human behavior in mind. Precautions must be taken to minimize errors and secure a safe cyberworld with the discussed methodologies and technologies.

Endnotes

1 IBM Global Technology Services, *IBM Security Services 2014 Cyber Security Intelligence Index*, May 2014, USA, *https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF*

2 IBM Security, *Cost of a Data Breach Report 2020*, 2020, *https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/*

3 Ponemon Institute LLC, *The Cost of Insecure Mobile Devices in the Workplace*, USA, March 2014, *http://www.ponemon.org/local/upload/file/AT%26T%20Mobility%20Report%20FINAL%202.pdf*

4 *Op cit* IBM Security

5 Verizon, *2020 Data Breach Investigations Report*, USA, 2020, *https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf*

6 *Security*, "Verizon 2020 Data Breach Report: Money Still Makes the Cyber-Crime World Go Round," 19 May 2020, *https://www.securitymagazine.com/articles/92415-verizon-2020-data-breach-report-money-still-makes-the-cyber-crime-world-go-round*

7 Howlett, T.; "Top Third-Party Data Breaches of 2020: Lessons Learned to Make 2021 More Secure," *DarkReading*, 7 December 2020, *https://www.darkreading.com/attacks-breaches/top-third-party-data-breaches-of-2020-lessons-learned-to-make-2021-more-secure/d/d-id/1339617*

8 Cimcor, "Change Control," *https://www.cimcor.com/cimtrak/features/change-control*