Humans and Cybersecurity—The Weakest Link or the Best Defense?

Cyberwar and conventional war have certain similarities, but cyberwar involves obscure and often anonymous enemies. Cybersecurity is one of the most significant challenges facing both enterprises and individuals today. It is vital to be prepared to defend against the war waged by sophisticated cyberadversaries.

Undeniably, the human factor plays an essential role in cybersecurity, and as one cybersecurity expert states, "People often represent the weakest link in the security chain and are chronically responsible for failure of security systems."[1] Meanwhile, the COVID-19 pandemic has led to a large increase in the number of remote workers, and there has been an uptick in sophisticated phishing email campaigns by cybercriminals taking advantage of fearware, which means exploiting the population's fears through a new type of cyberattack.[2] Hackers are posing as US Centers for Disease Control and Prevention (CDC) or the World Health Organization (WHO) professionals to lure unsuspecting users.

Surprisingly, public awareness of cyberattacks and cybersecurity remains inadequate. Even cybersecurity professionals can fall prey to some of the advanced social engineering tactics that exploit human psychological vulnerabilities.

Any casual behavior can potentially lead to information security leaks and cause irreparable damage. If an enterprise deploys technological solutions and policies to address cybersecurity issues but forgets to address employee awareness, its cybersecurity strategy may fail. People, technology and policies must be integrated to enhance an enterprise's overall security posture.

The human factor played a crucial role in the recent WannaCry ransomware epidemic. Equifax, Twitter, Capital One and the US Democratic National Committee incidents were also impacted by human-related data breaches. The UK Information Commissioner's Office (ICO) also revealed that 90 percent of the country's data breaches in 2019 resulted from human error.[3]

Legacy Security Solutions Are No Longer Effective

For a long time, enterprises have implemented various network solutions such as firewalls, intrusion detection, antivirus programs and other security tools to protect against threats originating from external sources. However, these commonly used security tools frequently fail to address insider threats arising from the human factor.

Users interact with both systems and security tools, and this interaction is the most significant security risk of all. The problem, according to one expert, is that:

> *...[P]eople don't understand computers. Computers are magical boxes that do things. People believe what computers tell them. People just want to get their jobs done. People don't understand risks.*[4]

Julien Legrand, CISA, CRISC, CISM, CCNA, CEH, CISSP
Is a cybersecurity architect at Thales, based in Hong Kong. He is a seasoned information security professional who is passionate about technology and cybersecurity, with a proven record of designing, implementing and continuously improving security controls in line with best practice and risk appetite. Legrand's areas of expertise focus particularly on identity and access management, cryptography, data protection and risk management. He works seamlessly with both technical and nontechnical stakeholders, and he is able to communicate with gravitas and clarity to ensure success.

Fortunately, emerging technologies such as zero trust and behavior-based analytics are helping enterprises reduce some human risk factors. With a limited amount of time to manage an increasing volume of alerts, security analysts can benefit from zero trust screening and user behavior analytics to prioritize alerts and dedicate their time to investigating anomalous user behavior.

However, technology is not the only solution; employee awareness is key. Humans can intentionally or unintentionally undermine any cybersecurity measure, posing a threat to the enterprise, its employees and its customers. People are often ignorant of the fact that they have access to sensitive data and systems and are unaware of the numerous risk factors associated with these information assets.

The Human Role in Ensuring Security

As the US National Institute of Standards and Technology (NIST) explains in its 2018 guidebook for National Cybersecurity Awareness Month, security depends on developing a cybersecure culture.[5] This kind of enterprisewide ethos emphasizes, reinforces and drives behavior.

NIST's main point is that enterprises require the right organizational mindset and suitable awareness programs to develop and maintain a cybersecure culture. Security is not only for security teams, because attackers will look for and exploit the weakest link in the enterprise. This means that everyone should champion the enterprise's security efforts.

> "SECURITY IS NOT ONLY FOR SECURITY TEAMS, BECAUSE ATTACKERS WILL LOOK FOR AND EXPLOIT THE WEAKEST LINK IN THE ENTERPRISE."

In practice, organizations should focus on employees, C-level executives, security specialists, boards of directors (BoDs) and human resources (HR) departments, determining the role each plays in protecting the enterprise from cyberattacks (**figure 1**).

Employees
Every employee is responsible for ensuring cybersecurity. All employees should know how to handle emails and how to respond to suspicious links and attachments from unknown senders. Enterprises should enforce policies for creating or changing passwords. All users must be aware of basic security actions, including regularly updating

Figure 1—Cybersecurity Responsibilities

Employees	• Be vigilant, report suspicious emails and links. • Comply with security policies.
C-Level Executives	• Embed security into the business DNA. • Take the lead on funding and endorsing cybersecurity.
Security Personnel	• Organize, design and implement security programs. • Proactively monitor and manage cyberthreats.
The Board	• Take oversight of cybersecurity strategies. • Authorize security budgets and initiatives.
Human Resources	• Set cybersecurity expectations for new employees. • Endorse controls to protect employee data.

operating systems and other installed software and antivirus programs. In addition, employees should update security software and encrypted channels to share sensitive information.

Finance department employees must maintain the confidentiality and integrity of sensitive financial information. Legal and compliance personnel can support security teams by ensuring compliance with dynamic regulations and privacy laws. All employees can champion security by reporting risk factors to the responsible teams to prevent incidents.

C-Level Executives

When cyberincidents occur, executive leadership is often blamed. For example, a few months after Target's cyberincident, its chief executive officer (CEO) resigned.[6] Similarly, Sony Pictures' cochair resigned within two months of an attack that leaked upcoming film releases, employee information and personal emails.[7] It was no surprise that the Equifax CEO was forced to quit within two weeks of the disclosure of its massive breach, and Imperva's CEO resigned after the enterprise reported a cloud data breach.[8]

Although regulations such as the EU General Data Protection Regulation (GDPR) do not hold an enterprise's directors and officers personally liable for data breaches, the Data Protection Bill introduced in the UK House of Lords in 2017 to supplement the GDPR clarifies that if an offense is committed through negligence or deliberately, the enterprise and the directors will be held legally responsible and will be subject to prosecution.[9]

In the US Senate, a bill was introduced to amend the US Federal Trade Commission Act to establish requirements and responsibilities for entities that use, store, collect or share personal information. The proposed bill recommends jail terms for CEOs who fail to disclose privacy violations.[10]

A 2018 report by Accenture shows that executives' growing support for cybersecurity is starting to pay dividends.[11] To ensure lasting success and realize the full benefits of investment in cyberresilience, the report recommends that C-level executives build on this momentum. Leaders would be well advised to keep pace with change and adopt breakthrough technologies, embedding cybersecurity into the fabric of their businesses. This will become even more important because a majority of CEOs whose enterprises experience data breaches will start to be held accountable by 2024, as both the severity and the frequency of cyberattacks grow worldwide.[12] Regulators and governments around the world will react promptly to serious incidents resulting from failures to secure systems. They will increase the rules and regulations governing cybersecurity, making it impossible for CEOs to plead ignorance or hide behind insurance.

> “LEADERSHIP IS A CRITICAL COMPONENT OF CYBERSECURITY, AND CEOS MUST MAKE IT CLEAR THAT EVERY STAKEHOLDER SHARES RESPONSIBILITY FOR ENSURING THE ENTERPRISE'S SAFETY.”

Leadership is a critical component of cybersecurity, and CEOs must make it clear that every stakeholder shares responsibility for ensuring the enterprise's safety. C-level executives must establish transparent and practical governance around the enterprise's cybersecurity practices. Along the same lines, senior executives should be role models, demonstrating to all employees the importance of implementing security best practices. In addition, C-level executives should take the lead when it comes to funding security projects and ensuring that risk assessments inform all their security strategies.

There needs to be a new kind of chief information security officer (CISO).[13] This unique C-level executive should be invited to discuss cyberrisk and cyberthreats with the BoD. These security leaders must be able to organize, design and implement cybersecurity programs that meet the needs of the enterprise. In addition, the CISO is responsible for infusing a culture of cyberresilience throughout the enterprise.

Security Specialists

Cybersecurity specialists provide security during the development, implementation and running of software systems, networks and data centers. These professionals search for vulnerabilities and risk factors in information assets and monitor and manage intrusion attempts. In addition, security experts suggest security tools and measures for

software and hardware, and they design strategies and defensive solutions to deal with external intruders and insider threats.

BoD

BoDs are recognizing that security failures can be catastrophic. Simply put, cybersecurity has become a priority in meeting overall business objectives, and it should not be left solely to the purview of the IT department. A cyberincident can ruin an organization's bottom line and cause enormous damage, including destroying brand reputation, undermining customer trust, reducing stock value and leading to noncompliance penalties.

Boards need to assume oversight of cybersecurity strategies. This entails significant changes in cyberresilience reporting and governance, with the board authorizing cybersecurity initiatives and budget allocations. This approach can fuel improvements.

Reports of sophisticated and frequent cyberincidents are an indication that BoDs should significantly increase security spending, both in absolute terms and as a percentage of IT budgets. Fortunately, there has been excellent progress in this area, with two-thirds of boards now having direct cybersecurity oversight, and boards and CEOs approving 59 percent of budget allocations as of 2018.[14]

It is also essential to have board members with cyberexpertise. In a recent interview, Bob Zukis, the founder and CEO of the Digital Directors Network, noted that:

> *By not having the right technology skill sets in every boardroom, companies want their boards to set themselves up for failure, so it's almost guaranteed to get worse before it gets better.*[15]

A growing number of organizations plan to recruit directors with technology expertise to help address escalating cybersecurity threats.[16]

HR

HR personnel typically introduce new employees to an enterprise, and they should communicate security expectations right from the start. HR should also collaborate with security teams to organize and run security training during employee orientation and implement ongoing cybersecurity awareness programs for staff.

The HR department also needs to collaborate with frontline management to ensure that employees follow all security procedures and policies. Frontline managers work with employees on a day-to-day basis, and liaising with the HR team can gain an edge in the fight against cyberresilience.

At the same time, HR departments hold sensitive employee information and are, therefore, responsible for implementing reliable security controls to prevent unauthorized access to or modification of these data.

When employees leave the enterprise, HR should ensure that all enterprise devices are returned, accounts are closed and credentials are revoked. This prevents ex-employees from jeopardizing the enterprise's security by using active passwords after their exit.

Conclusion

Organizations require the right mindsets and suitable awareness programs to develop and maintain cybersecure cultures. They can achieve this objective by involving every stakeholder in security initiatives.

In practice, enterprises should focus on employees (who must be taught to handle emails carefully and protect sensitive information), C-level executives (who should take the lead on funding security projects), security specialists (who ensure security in software, networks and devices), BoDs (which oversee cybersecurity strategies) and HR departments (which communicate security expectations to employees). Each group plays a role in ensuring that the enterprise is safe from cyberattacks.

Humans can also augment a variety of security tools and practices to enhance the capabilities of a robust cybersecurity program. In this way, organizations can transform and develop new, digitally enabled opportunities while effectively managing potential attack surfaces.

Security should become business as usual—a priority embedded in the fabric of an enterprise—not an afterthought.

> “HUMANS CAN ALSO AUGMENT A VARIETY OF SECURITY TOOLS AND PRACTICES TO ENHANCE THE CAPABILITIES OF A ROBUST CYBERSECURITY PROGRAM.”

Endnotes

1 Schneier, B.; *Secrets and Lies: Digital Security in a Networked World*, Wiley, USA, 2000, *https://www.oreilly.com/library/view/secrets-and-lies/9781119092438/28_chapter17.html*

2 Pacag, H.; “Multiple Phishing Attacks Discovered Using the Coronavirus Theme,” Trustwave, 13 February 2020, *https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/multiple-phishing-attacks-discovered-using-the-coronavirus-theme/*

3 Bisson, D.; “7 Data Breaches Caused by Human Error: Did Encryption Play a Role?” Venafi, 15 October 2020, *https://www.venafi.com/blog/7-data-breaches-caused-human-error-did-encryption-play-role#:~:text=Human%20error%20has%20a%20well,87%25%20the%20previous%20two%20years*

4 *Op cit* Schneier

5 National Initiative for Cybersecurity Education Working Group, National Institute of Standards and Technology (NIST), *Cybersecurity Is Everyone’s Job*, USA, October 2018, *https://www.nist.gov/system/files/documents/2018/10/15/cybersecurity_is_everyones_job_v1.0.pdf*

6 NeSmith, B.; “CEOs: The Data Breach Is Your Fault,” *Forbes*, 26 June 2018, *https://www.forbes.com/sites/forbestechcouncil/2018/06/26/ceos-the-data-breach-is-your-fault/?sh=7981461958b0*

7 Raftery, L.; “Sony Pictures Co-Chair Amy Pascal to Step Down in Wake of Hacking Scandal,” *TV Guide*, 5 February 2015, *https://www.tvguide.com/news/amy-pascal-sony-pictures-resigns-fired/*

8 Kobialka, D.; “Imperva CEO Resigns Following Data Breach,” MSSP Alert, 28 October 2019, *https://www.msspalert.com/cybersecurity-talent/imperva-ceo-resigns*

9 Hancock, B.; “What Does GDPR Mean for Senior Management?” *BusinessWest*, 7 March 2018, *https://www.businesswest.co.uk/members/blog/what-does-gdpr-mean-senior-management*

10 Wyden, R.; Consumer Data Protection Act—Discussion Draft, 115th Congress, 2nd Session, *https://www.wyden.senate.gov/download/11012018-wyden-privacy-bill-discussion-draft*

11 Accenture, *Gaining Ground on the Cyber Attacker: 2018 State of Cyber Resilience*, 2018, *https://www.accenture.com/t20180416T134038Z__w__/us-en/_acnmedia/PDF-76/Accenture-2018-state-of-cyber-resilience.pdf#zoom=50*

12 Bestpractice.biz, “CEOs to Be Held Accountable for Data Breaches by 2024,” 7 September 2020, *https://bestpractice.biz/ceos-to-be-held-accountable-for-data-breaches-by-2024/*

13 *Op cit* Accenture

14 Talley, K.; “CEOs Are Taking More Responsibility for Cybersecurity Protection,” *FierceCEO*, 25 April 2018, *https://www.fierceceo.com/technology/ceos-are-taking-more-responsibility-for-company-s-cyber-security-protection*

15 Ferracone, R.; “Good Governance: Do Boards Need Cyber Security Experts?” *Forbes*, 9 July 2019, *https://www.forbes.com/sites/robinferracone/2019/07/09/good-governance-do-boards-need-cyber-security-experts/?sh=289355961859*

16 Rathod, L.; “Why Should You Have a Cybersecurity Expert Sitting on Your Board of Directors?” Diligent, 20 April 2018, *https://diligent.com/en-gb/blog/why-should-you-have-a-cybersecurity-expert-sitting-on-your-board-of-directors/*