Exploitable Traits as Vulnerabilities

The Human Element in Security

日本語版も入手可能

www.isaca.org/currentissue

As the saying goes, every chain is only as strong as its weakest link and, in the case of information security, that weakest link is the human factor. Employees are high-level risk factors at all enterprises.[1] According to the Verizon *2020 Data Breach Investigation Report*, 67 percent of successful cyberattacks are the result of human negligence or human-based attacks, such as phishing.[2] Other statistics reveal that 98 percent of cyberattacks are based on human factors and social-engineering techniques.[3] These data underscore that human vulnerabilities help attackers gain access to targeted systems, engage in spear phishing, spread malware, exploit other vulnerabilities of IT systems and employ social-engineering methods.[4]

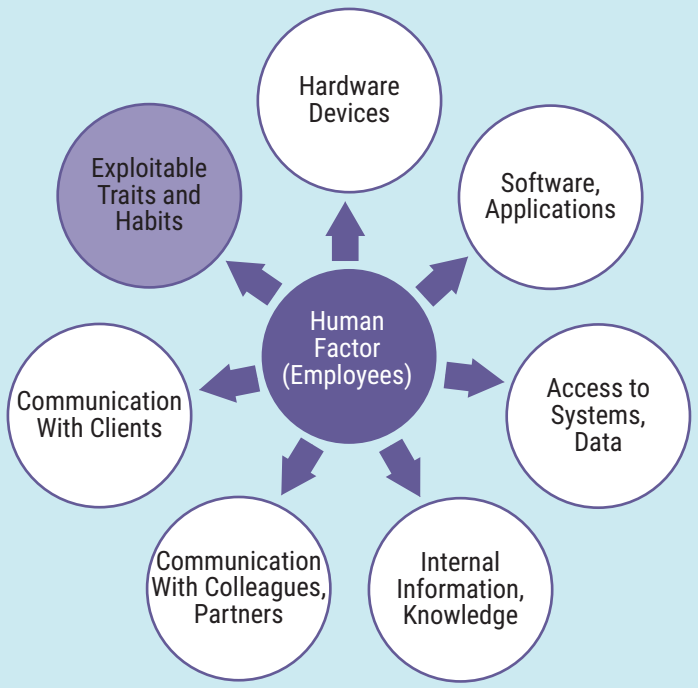
As one author wrote, "Cybersecurity is more than bits and bytes, it's also people and process."[5] Employees are useful resources for cyberattackers because they have direct access to all the assets an enterprise wants to protect (**figure 1**). Employees use and transport hardware devices (e.g., notebooks, pen drives); install and update software and work with applications; have access to important files, systems and data; possess useful internal information and knowledge; communicate with one another, clients and partners; and have exploitable traits that make them attractive targets of social-engineering attacks.[6]

Exploitable Human Traits, Habits and Situations

People have many traits and habits that can be easily exploited by cyberattackers. For example,

Eszter Diána Oroszi, CISA, CRISC, CISM
Is a lead consultant at a Hungarian information security consulting enterprise. She has 12 years of experience in the field of information security, with a special interest in human-based attacks, social engineering audits and security awareness improvement. She is a Ph.D. student at National University of Public Services (Budapest, Hungary), and her research area is measuring and improving the security awareness level of users using gamification.

Figure 1—Employees' Connection to Workplace Assets



helpfulness is one of the most basic human traits that social engineers can exploit in countless ways. Similarly, curiosity, credulity and naivety can be leveraged to carry out phishing attacks and spread malware. Attackers can also take advantage of users' inattention, negligence or ignorance. Attackers select the perfect targets by identifying and analyzing their traits, characteristics, behaviors, skills or knowledge and then creating situations to exploit them.

"A personality trait is a characteristic pattern of thinking, feeling, or behaving that tends to be consistent over time and across relevant situations."[7] Personality analysis and profiling are used often by psychologists and human resources (HR) departments to solve problems, improve or utilize skills, or identify the right career path for people. There are several methods of analyzing personality:

- Goldberg's "Big Five" model divides human traits into five groups: extraversion, agreeableness, conscientiousness, neuroticism and openness to experience (with a change in order, this is also called the OCEAN model).[8]
- Marston's DiSC model comprises four categories: dominance, influence, stability and conscientiousness.[9]
- The Myers-Briggs type indicator uses opposite word pairs—extraversion or introversion, sensing or intuition, thinking or feeling, and judging or perceiving—to define four groups and then combines them to identify 16 different personality types.[10]
- Mann's method defines four personality profiles—driver, expressive, analytical and amiable—and maps them to typical workplace roles. For example, management is usually results driven (driver), researchers and those working in finance are mostly safety driven (analytical), employees in the marketing department might be ego driven (expressive), and clerks and administrators are usually comfort driven (amiable).[11]

> "ATTACKERS SELECT THE PERFECT TARGETS BY IDENTIFYING AND ANALYZING THEIR TRAITS, CHARACTERISTICS, BEHAVIORS, SKILLS OR KNOWLEDGE AND THEN CREATING SITUATIONS TO EXPLOIT THEM."

Mann's method can be useful for understanding employees' vulnerabilities and human-based risk factors. If attackers know the motivations, drivers and general characteristics of each role, they can exploit these traits. However, if employers are aware of these personality types and the associated risk factors, they can identify the most appropriate risk-mitigating actions and take the required steps to improve security awareness.

Exploitable traits and habits can be divided into four main categories: personal, workplace, momentary and situational (**figure 2**).[12]

These four categories of traits can be related, and they often intersect. Such combinations can be exploitable by social engineers. For example, if a new employee who is helpful and who often communicates with unknown customers is on vacation, an attacker can contact them by phone,

Figure 2—Categories of Human Traits and Examples of Exploitable Situations

Personal	Workplace	Momentary	Situational
Helpful	New employee	Tired	Conflict averse
Naive	Daily routine tasks	Hurriedness	Reckless
Curious	Problem-solving skills	Haste	Reflexive
Open	Working with unknown people (e.g., clients, colleagues)	Inattentive	Frightened
Impressionable	Dissatisfaction	Holidays	Avoiding liability
Shy	Affordability	Vacations	Compromising
Negligent	Extortion	Sick leave	Cooperative
Enthusiastic	Rivalry	Fair	Angry

impersonating a client and asking for sensitive information. Because the employee is new to the job and would like to get a good performance review, they might fall for the trick and provide the requested data, especially if they have no routine for checking invalid requests and lack security awareness.

Personal Traits

Personal traits are the most basic human characteristics. All people have them, and they are usually very difficult or even impossible to change. Examples include helpfulness, curiosity and openness, which are some of the most common traits exploited by social engineers. Helpfulness is useful when attackers want to gain entrance to a building or when they employ personal deception over the telephone. Curiosity can be used to exploit targets and spread malware or carry out phishing attacks.

Workplace Characteristics

Certain traits and situations are related to a given workplace or position within an enterprise. Based on working conditions, these traits might change over time, such as when a person changes positions, tasks or projects. New employees can be attractive targets for attackers because they are not yet familiar with all their colleagues and can easily be victims of deception, fake requests via the phone or email scams. However, this is a temporary state: As the new employee integrates into the enterprise, the probability of a successful attack decreases.

Other popular targets of social-engineering attacks are people who do routine work, such as customer service representatives, because it may be difficult for them to filter out fake requests. For example, someone working every day with Excel files that contain macros might be unable to detect a suspicious or deceptive attachment that contains macro-based malicious code. In addition, employees who are often in contact with unknown individuals (e.g., employees of partners, clients) or know coworkers at other work sites only by phone or email are vulnerable, especially if they are helpful or inattentive. Unusual requests, phone or email scams, or even personal attacks might be successful against these targets.

Negative attitudes such as dissatisfaction with working conditions and salary can also be connected to this category and can be exploited in extreme cases to commit crimes such as bribery and extortion. It is important that workplace characteristics and personal traits be aligned when certain qualities are required or advantageous in employees who are filling specific positions.

Momentary Traits

These traits are usually short lived and can change quickly, depending on conditions. For example, an employee may be tired after putting in a lot of overtime, leading to inattention. When someone goes on vacation or takes sick leave, attackers can exploit both the absent worker and the substitute. Attackers can call workers during their vacation and demand that they solve a problem quickly or fulfill a request immediately; assuming the worker wants to solve the task quickly, attackers may be redirected or connected to substitutes. In some cases, attackers might try to gather useful internal information via the automatic replies of absent workers (e.g., contact information of substitutes, projects, tasks). This situation is exploitable when the substitute does not verify the authenticity of a request or does not want to bother the absent colleague or the appropriate superior.

A common feature of these momentary traits is that they are intermittent, lasting for a few days or weeks, and then disappear as circumstances change. If attackers can identify the existence of these traits or the situations connecting them, or if attackers can find an employee exhibiting one of

these traits, they can create an attack scenario to exploit the target.

Situational Traits

Situational traits are momentary traits that generally occur during a stressful situation, such as a security breach. They are considered separately because they usually do not help an attacker take offensive action but rather they affect the execution of an attack after it is detected. One example is if an employee identifies a suspicious event—an outsider walking into the building without an escort or a badge—but does not question the visitor (or intruder) or report the event to security guards, hoping to avoid conflict in case nothing is wrong. For telephone scams, targets' reflex reactions can be useful to attackers, such as when the social engineer poses as an employee of the help desk and scares the target by saying that their password has been compromised and must be changed immediately. The frightened victim reveals the password without thinking about it (this works especially well after a phishing attack). Avoiding liability could lead to malware infection, where the affected user tries to explain that antimalware software is installed and it should have identified the malicious code.

Improving Employees' Security Awareness

Employees may be the targets of cyberattacks, but they are also the first line of defense, sometimes called the "human firewall." Well-trained and security-aware employees can prevent, detect and report security events and incidents. Technological countermeasures such as firewalls, antimalware software and strict access rights are not sufficient defenses against social engineering attacks.[13] Employees can ignore or even bypass these measures, and they can create a false sense of security. For example, users may open links or attachments in suspicious emails because they believe that antimalware software will detect any malicious codes and actions. The only effective solution is to improve the security awareness of users and sensitize them to the topic. Each enterprise must develop its own security awareness program tailored to its environment to prevent human-based attacks such as scams, fraud, phishing or even physical intrusion.

Security awareness training should include more than the standard training materials, such as posters, newsletters or gifts. It should highlight real problems, such as presenting the results of tests and audits, and it should include gamified program elements.[14] The main purpose of security awareness training is to inform employees of their responsibilities based on information security policies and applicable regulations. This includes explanations of why these rules are necessary, what kinds of cyberattacks and social-engineering techniques exist, and how employees can collaborate to reduce human-based risk.

> "THE BEST INFORMATION SECURITY TRAINING IS TAILORED TO THE TARGET AUDIENCE, TAKING INTO ACCOUNT ITS DIFFERENT ROLES, RESPONSIBILITIES, ROLE-SPECIFIC HUMAN TRAITS AND HABITS, WORKPLACE SITUATIONS, AND MOTIVATIONS."

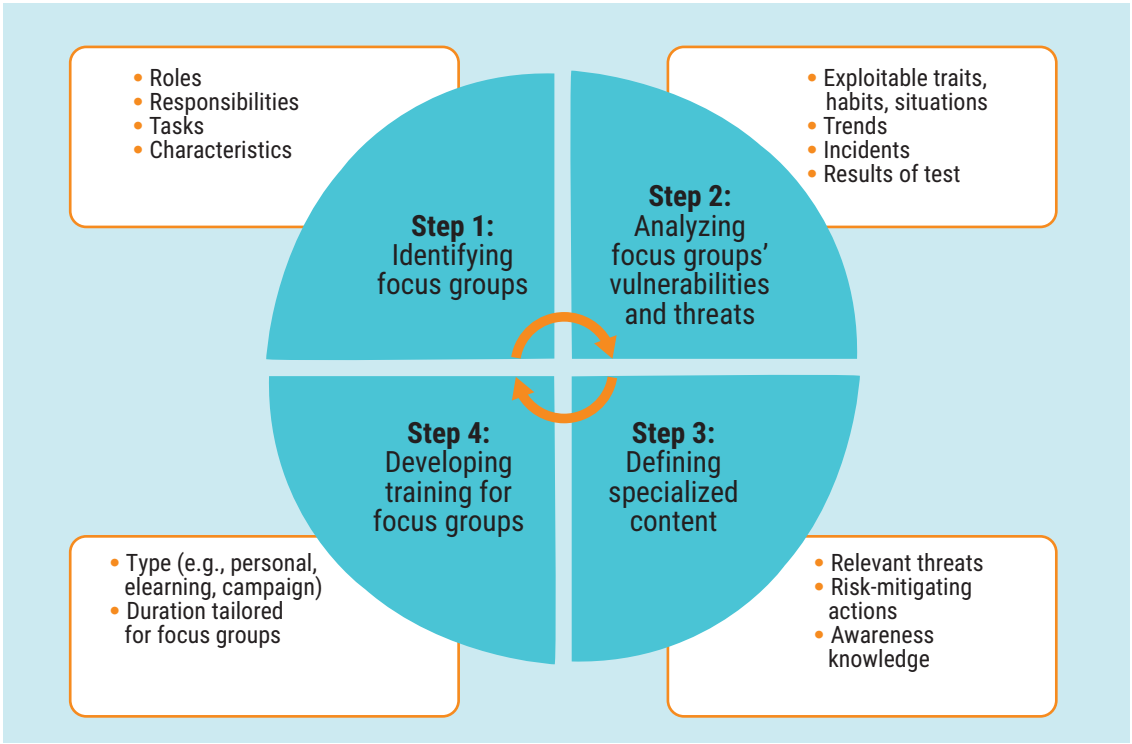
The best information security training is tailored to the target audience, taking into account its different roles, responsibilities, role-specific human traits and habits, workplace situations, and motivations. Therefore, training materials and the educational framework should be customized for particular user groups. **Figure 3** illustrates how to develop a specialized security awareness training program. In step 1, the enterprise identifies focus groups based on workplace roles and responsibilities and special characteristics and personality. Suggestions for defining focus groups include:

- Management
- Users who communicate often with unknown people (e.g., administrative assistance, marketing or communications departments, customer service, reception)
- Users who perform routine work (e.g., administrators, front-office workers, help desk)
- Users who have privileged rights (e.g., system operators, IT administrators)
- Back-office workers and employees in other areas and departments (e.g., lawyers, financial experts, developers, analysts) using subdivided, specialized training material if possible
- New employees

Enjoying this article?

- Read *A Holistic Approach to Mitigating Harm From Insider Threats. www.isaca.org/insider-threats*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Figure 3—Security Awareness Training



In step 2, the enterprise analyzes the weaknesses in each of the focus groups: threats, vulnerabilities and exploitable human traits, habits and situations. In addition, countermeasures based on trends, past security incidents and events, and the results of security awareness measurements should be considered to reduce risk. Measuring the level of security awareness on a regular basis is important not only to determine the efficiency of training, but also to create specialized educational materials highlighting weaknesses, risk factors and actual problems. Inputs can come from past security incidents within the enterprise itself or around the world, questionnaire-based awareness tests, observation, or results of social-engineering audits.

Based on the results of step 2, step 3 is used to define the most important knowledge for each focus group. Specialized materials help participants better understand real threats and attack types and use protection and detection methods more effectively. The topics and the depth of content may be different in each focus group, depending on the participants' roles, responsibilities, workplace characteristics and typical threats. In addition to presenting human-based attacks, threats, and preventive and defensive actions, the training material should cover the user's role in information security and the advantages of security awareness. Step 4 is used to determine the training method and duration of training based on the targeted groups. Training methods include:

- Personal education or presentation
- Self-study elearning
- Interactive workshops
- Awareness campaign elements

If users have had no awareness training, in-person training is most useful. If the training is a refresher course, elearning or a shorter presentation focusing only on actual threats might be appropriate. In the case of exceptional training (e.g., after a real attack), campaign elements such as newsletters or blog posts might be used. It is also recommended to identify and assess the demands and requirements of the target audience and plan to use methods based on the audience.

A first-time training program generally takes 1–2.5 hours, depending on the group or the topic, if the structure is not modular. In the case of a modular structure, each training session should take no

more than 30–45 minutes and should be held on a monthly or quarterly basis. Training of management usually takes 30–45 minutes, emphasizing the threats affecting managers and the special supportive and exemplary nature of their roles.

Security awareness campaigns such as Cybersecurity Month or Cybersecurity Week can complement training sessions. They help users maintain their security awareness and remember what they learned during training and why security is important, and they can even provide opportunities to gain practical experience. Security awareness campaigns and programs can include training sessions, special presentations, posters, screensavers about information security rules, newsletters, blogs, gifts, quizzes, and online or offline games to draw attention to attacks that exploit the human factor. People seem to prefer interactive program elements such as mobile applications or security awareness escape rooms.[15] According to feedback from users, more traditional elements (e.g., posters, newsletters, screensavers) provide mainly unnecessary information or common-sense instructions, making them less effective methods of improving security awareness.

A successful security awareness program teaches participants to recognize their own vulnerabilities and exploitable traits and habits. This helps them protect themselves against malicious social-engineering attacks.

Conclusion

Employees are important elements of information security—not only as potential targets of attacks but also as human firewalls. To avoiding becoming victims, users should know their weaknesses, exploitable traits and bad habits and recognize which types of attacks can take advantage of their vulnerabilities. In a working environment, some user groups have specific, commonly known exploitable traits and characteristics, which is why it is important to tailor security awareness programs to these employees, focusing on their vulnerabilities. After completing a well-constructed, targeted security awareness training program, workshop or campaign, participants will be more likely to follow the rules and practice good security-aware behavior.

"A SUCCESSFUL SECURITY AWARENESS PROGRAM TEACHES PARTICIPANTS TO RECOGNIZE THEIR OWN VULNERABILITIES AND EXPLOITABLE TRAITS AND HABITS."

Endnotes

1 Mitnick, K. D.; W. L. Simon; *The Art of Deception: Controlling the Human Element of Security*, Wiley, USA, 2003
2 Verizon, *2020 Data Breach Investigations Report*, USA, 2020, *https://www.cisecurity.org/wp-content/uploads/2020/07/The-2020-Verizon-Data-Breach-Investigations-Report-DBIR.pdf*
3 PurpleSec, "2021 Cyber Security Statistics: The Ultimate List of Stats, Data and Trends," USA, 2021, *https://purplesec.us/resources/cyber-security-statistics*
4 Nobles, C.; "Botching Human Factors in Cybersecurity in Business Organizations," *Holistica,* vol. 9, iss. 3, 2018, p. 71–88
5 Fandi, A.; "Cybersecurity Is More Than Bits and Bytes, It's Also People and Process," LinkedIn, 30 September 2019, *https://www.linkedin.com/pulse/cybersecurity-more-than-bits-bytes-its-also-people-process-fandi*
6 Oroszi, E. D.; "Social Engineering Techniques: Targeted Cyberattacks," National University of Public Services, Budapest, Hungary, 2018
7 Soto, C. J.; "Big Five Personality Traits," *The Sage Encyclopedia of Lifespan Human Development,* Sage, USA, 2018
8 *Ibid*.
9 Inscape Partners, "The DiSC Model," *https://ipbpartners.eu/public/artikkel/DiSC_theory__background.pdf*
10 Erős, I.; M. Jobbágy; "A Myers-Briggs Tipus Indikátor (MBTI) Magyarországon," *http://www.mentalhub.hu/mbti.pdf*
11 Mann, I.; *Hacking the Human*, Gower, UK, 2008
12 *Op cit* Oroszi
13 *Op cit* Mitnick
14 *Op cit* Oroszi
15 Oroszi, E. D.; "Make Security Awareness an Experience," ISACA Now, 25 September 2020, *https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/make-security-awareness-an-experience*