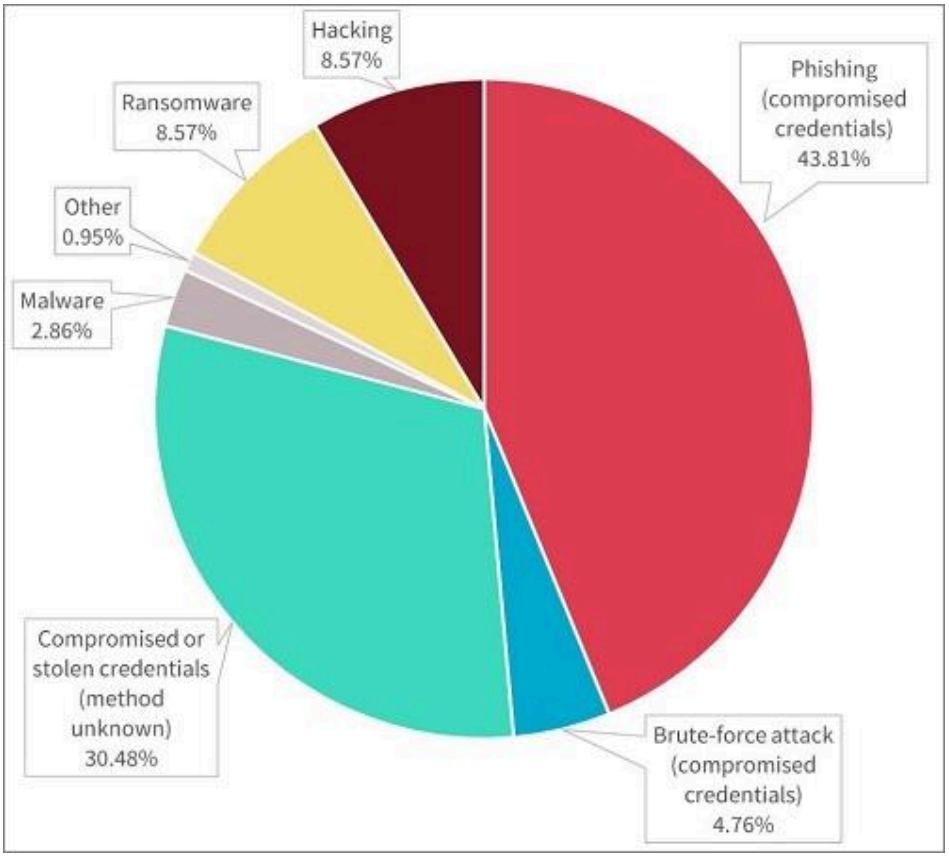
Human Factors

Question 1: Identify security gaps or opportunities in training related to human factors

Potential gaps or opportunities in training(s) related to human factors is immense. But first to identify these gaps, understanding what human factors that lead to potential breaches is important. Human error is the most common reason for breaches within a company. For example, phishing emails, not following company policy, or employees being negligent to peripheral devices. Many breaches can be prevented if employees have a proactive cybersecurity mindset and this starts with proper training. In a 2023 study conducted by Verizon's Data Breach Investigations Report (DBIR), it states that 74% of cyber breaches can be attributed to human error (Peters, 2023), (See Figure 1 for a breakdown of breach sources).



(Figure 1, Human error the leading cause of data breaches, 2019)

Creating a proactive cybersecurity culture between employees on all levels of the company is important and can be a major advantage or costly setback for an organization. Solutions that can be implemented are feedback surveys or role-specific workshops. Employees not being thoroughly trained regarding cybersecurity and company policies can be a difference between the company growing or the company having to pay possibly millions of dollars in ransom or a negative reputation.

Another gap or opportunity in training(s) related to human factors could be addressed is employee burnout/stress. Oftentimes repetitive tasks or impractical policies can attribute to employees lack of motivation and breach of company policies. The combination of employees facing barriers and impractical policies within their roles that can lead to cognitive overload. Rather than relaxing standards, organizations should collaborate with employees to develop practical, effective policies. Understanding the struggles employees are facing is important and should be taken into account when creating strong and effective policies for the company. Conversing and understanding employees' struggles is a good first step in creating and fostering a strong security environment and policies. A proven framework that has been implemented by many companies through the industry is the Human-Centric Cybersecurity Framework.

The Human-Centric Cybersecurity Framework prioritizes intuitive systems, targeted training, and positive reinforcement to align security measures with human behavior (Keepnet, 2025). It has shown great promise and the collaboration between both the security team and employees has built strong foundations for developing proactive security environments.

Legal Factors

Question 2: Identify security gaps or opportunities in training related to legal factors

Security gaps or opportunities in training related to legal factors can vary. Common gaps include insufficient audit documentation, incomplete coverage of legal mandates, and lack of role-specific training on legal responsibilities. I can speak from personal experience that many of these topics are briefly discussed, if they are even discussed at all. These topics solidify the groundwork of an organization's legal obligations. Taking shortcuts to legal compliance puts the organization at serious risk. Educating employees on the roles they contribute to the organization following legal guidelines should be a focus in the training procedures of the company. The employees play a big role in the company following legal regulation and they should know that.

All too often, companies overlook legal obligations in employee training which can lead to the company being fined or shut down all together. A recent example of this was Equifax in 2017 when they failed to follow cybersecurity regulations which ultimately led to the company paying millions in legal fees and suffering reputational damage. In 2017 Equifax went against legal regulation and decided to not patch a known vulnerability within their Apache Trust software, ultimately leading to 147 million individuals personal information being leaked. Personal information like social security numbers, addresses, and birthdates were all leaked because of their failure to follow legal regulation (Fourrage, 2024).

Not properly following or explaining legal regulation can lead to immense damage to the company and ultimately the consumer. Employees at all levels—from IT to HR and operations—must understand the laws and standards relevant to their roles. To build a strong proactive security environment, finding ways to inform employees of these laws need to be implemented. Providing interactive and educational workshops, real world, internal newsletters, and scenario-based training are examples of good ways to keep employees up to date and engaged with current legal factors that could impact the company.

Equipping all staff with this knowledge not only reduces the risk of breaches but also reinforces a culture of proactive security and legal responsibility within the organization.

Proactive Security Mindset

Question 3: Explain why a proactive security mindset is beneficial for all levels of the organization

A proactive security mindset at all levels is essential to identify and defend against vulnerabilities before they are exploited. It is important that employees on all levels within the organization play a part in helping make sure company information is secure. Entry level and early career employees play an important role in protecting the company. In 2016 Snapchat dealt with a security breach through a phishing attack. Employees within the HR department clicked on an email link that appeared to be from their CEO that led to reputation damage, employee data being compromised, and many other negative impacts (Hern, 2016). Employees on all levels within an organization can fall victim to cyberattacks if they are not properly trained and vigilant. It is important for routine training workshops/sessions to take place to build strong security infrastructure.

The incident related to Equifax's and Snapchat's security breach shows how important security protocols are for an organization. Because threats can approach from any direction- Executive to entry level- having employees understand policies is essential. Properly educating employees on policies in place will build a proactive security environment and trust with employees, consumers, and stakeholders.

References

- Fourrage, L. (2024, June 5). *What are the consequences of non-compliance with cybersecurity regulations?* Nucamp. Retrieved August 31, 2025, from https://www.nucamp.co/blog/coding-bootcamp-cybersecurity-what-are-the-consequences-of-noncompliance-with-cybersecurity-regulations
- Hern, A. (2016, March 29). *Snapchat leaks employee pay data after CEO email scam*. The Guardian. Retrieved August 10, 2025, from https://www.theguardian.com/technology/2016/feb/29/snapchat-leaks-employee-data-ceo-scam-email
- Peters, J. (2023, December 23). *Human error is responsible for 74% of data breaches*. InfoSec. Retrieved August 10, 2025, from https://www.infosecinstitute.com/resources/security-awareness/human-error-responsible-data-breaches/#:~:text=Human%20error%20is%20responsible%20for%2074%25%20of%20data%20breaches,-November%2030%2C%202023&text=The%20number%20of%20cybersecurity%20incidents,and%20help%20protect%20your%20organization.
- Tonkin, C. (2019). Human error the leading cause of data breaches [Photograph]. InformationAge. https://ia.acs.org.au/article/2019/human-error-a-leading-cause-of-data-breaches.html

- (2024, December 8). *Equifax Data Breach Explained: A Case Study*. Breachsense. Retrieved August 10, 2025, from https://www.breachsense.com/blog/equifax-data-breach/