**The Human Factor Causing Cyber Attacks**

When we talk about cyber security breaches, it is estimated that approximately [95% of them](https://media.scmagazine.com/documents/82/ibm_cyber_security_intelligenc_20450.pdf) are a result of human error and negligence. In other words, if there was no human error, about 19 out of 20 security breaches would not have occurred. It is human nature to make mistakes and learn to grow out of them. However, in cybersecurity these mistakes should not be overlooked due to the consequences that lie ahead.

According to a study of over 5,000 businesses conducted by B2B International and Kaspersky Lab, 52% of them believe that their business faces risk from insider threats. Their employees intentionally or unintentionally put their businesses at risk due to their negligent behavior.

Let’s take a look at how human error can cause cyber-attacks and why security awareness training is important to mitigate this threat.

**Human Error and Cyber Attacks**

In the context of cyber security, human error refers to unintentional bad decision or action by an employee that results in a potential security breach. These actions range from downloading malware-infected files to using a weak password. With workplaces getting more complicated and advanced, it becomes harder to manage countless usernames and passwords. If employees are not provided secure solutions, they start to take shortcuts to make work management easier for themselves.

**Types of Human Error in Businesses**

In terms of cybersecurity in a business setup, human error can be broadly divided into two categories i.e. decision-based and skill-based errors. Decision-based errors are a result of making a wrong decision, mostly due to lack of knowledge or not having enough information about the situation being faced. On the other hand, skill-based errors are a result of making a small mistake or temporary lapse due to a distraction or laziness, despite being aware of the correct course of action.

Let’s look at how these two categories can relate to different kinds of human errors that can jeopardize a business’s cyber security.

**Misdelivery**

It happens when an employee sends critical information to the wrong recipient. According to a [2018 report by Verizon](https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf), misdelivery was ranked at number five for the most common causes of cybersecurity breaches. One such incident occurred when an NHS employee revealed the names and email addresses of [more than 800 patients](https://www.bbc.co.uk/news/technology-36247186) who visited HIV clinics. The employee sending an email notification to all the patients chose the “To” option instead of “BCC” option and revealed the email addresses of all patients to each other. This is a real-life example of skill-based error where the employee knew the correct course of action but still made a minor mistake that resulted in a large-scale data breach.

**Password Mismanagement**

Creating strong and unique passwords still remains a challenge for many. According to a [report](https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security) published in 2019 by National Centre for Cyber Security, 123456 still remains to be the most commonly used password. Moreover, about 45 percent of people use one password for multiple accounts. Employees who have never received security awareness training tend to make many other mistakes such as sharing them with coworkers or writing them down on post-it notes.

**Using Unpatched software**

Whenever a vulnerability is discovered in a software, software developers fix it and send out the latest patch to their users to install it before they can be exploited by cyber criminals. This is the reason why it’s so important for all users to install security updates on their systems as soon as they arrive. Despite available patches, many users keep using unpatched software and expose their organization to cyber-attacks. The WannaCry ransomware attack in 2017 that affected thousands of computers all over the world used an exploit that was patched by [Microsoft](https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010) months before the attack.

**Physical Security Negligence**

Although security breaches are mostly attributed to cyberattacks, a data breach can also occur as a result of physical security negligence. If security of the premises is compromised, anyone with malicious intent can access your location physically and steal important information. The most common way of leaving your confidential data for physical access is by leaving documents on your desk, or throwing away old documents in trash without shredding them.

**Why is Security Awareness Training Important and How to Prevent Human Error?**

We now know that employees are the weakest link in cyber security breach incidents. If they are not well informed and don’t know about correct actions to take in certain situations, human error will continue to take place in organizations. It is essential to conduct regular security awareness trainings to enable employees to make knowledgeable and correct decisions during routine tasks and in times of ambiguity.

Here’s how you can train your employees and prevent them from making mistakes that can result in a potential data breach.

**Train Employees on Security Basics**

If you indulge too deeply in security concepts, your employee may lose interest. This is especially true for employees of non-technical departments. Train them about core concepts and security measures in routine tasks such as email handling, phishing scams, malware, internet and social media usage, physical workspace maintenance, password best practices and the use of multi-factor authentication.

**Stay Relevant and Engaging**

You don’t want to make your employees fall asleep with monotonous boring content. Keep them engaged by designing interactive training content that includes images and videos.

**Conduct Regular Training Sessions**

Humans have a tendency to forget. Even if you have conducted security awareness training for your employees, it is likely that they will forget the best practices after a certain time period. It’s important that these training sessions are conducted bi-annually or at least annually, to remind them how to stay vigilant. Educate them on best practices and security basics to allow them to make better decisions and take further guidance if they are not sure of what action to take under certain circumstances. Also conduct simulation exercises with them to prepare them for real attacks and use posters or monthly email brochures to keep reminding them about potential security risks.

**KMTech’s Cyber Security Vulnerability Assessment**

With KMTech’s cyber security Vulnerability Assessment, you can get a complete insight into your security vulnerabilities and deal with potential threats that could arise as a result of human error or negligence. Find out more about our vulnerability solution by signing up for a free Cyber Security Vulnerability Assessment with us [here](https://kmtech.com.au/book-a-cyber-assessment/).