**Cyber Security Risks: Human Factors Or Human Failures?**

* METACOMPLIANCE MARKETING TEAM
* AUGUST 9, 2021
* [CYBER SECURITY AWARENESS](https://www.metacompliance.com/blog/category/cyber-security-awareness/), [SECURITY AWARENESS TRAINING](https://www.metacompliance.com/blog/category/security-awareness-training/)



The ‘human in the machine’ is a fundamental consideration when creating an effective strategy to minimise cyber security risk. However, there are many aspects to this statement, as our employees are a vital part of the success of our organisation; instead of apportioning blame, we must tease out the malicious from the accidental, detecting the former and preventing the latter.

Through focused Security Awareness Training, human factors that lead to human failures can be mitigated. Here is how and why cyber security risk can be managed through an awareness of security.

**Why Human Factors Lead to Cyber Security Risk**

The human factor in cyber security risk is usually termed ‘insider threat’. The ‘insider’ takes the form of employees and non-employees, such as consultants. The simple fact that insiders are an integrated part of an organisation’s processes and utilise IT resources with permission, makes it difficult to address the human failures that lead to cyber security risk.

Insider-related cyber security risk is a major problem: a [2020 Insider Threat Report by cyber security Insiders](https://www.cybersecurity-insiders.com/wp-content/uploads/2019/11/2020-Insider-Threat-Report-Gurucul.pdf) points out that 68% of organisations feel “moderately to extremely vulnerable” to insider threats. This is not surprising when you look at some of the breaking news cyber attack headlines of the last year, such as the [Twitter](https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html) hack of 2020, where high-profile Twitter accounts, including Barack Obama’s, were accessed and used to trick Twitter users into performing illicit bitcoin transactions. Losses are estimated to be around $180 million (£129 million) and 4% was wiped off Twitter’s share price. The hack involved spear-phishing Twitter employees and stealing privileged credentials.

Human factors are used by cybercriminals to effect unauthorised access, steal credentials, and infect IT systems and endpoints with malware such as ransomware. Without the human-in-the-machine effect, cybercrime would be much more difficult.

**The Human Factors That Lead to Human Failures**

According to [research from IBM](https://www.ibm.com/security/data-breach/threat-intelligence), the top three areas to focus attention on when creating security strategies to mitigate cyber security risks are:

1. Phishing
2. Scan and exploit
3. Unauthorised use of credentials

All three vectors have an element that involves a human factor at some point in the attack chain.

**Phishing and Spear-phishing – human factors:** This requires a human target to click on a link or open an infected attachment to begin the infection chain. Often, phishing will be used to target privileged users (spear phishing) to harvest their credentials. Privileged users have access to more important resources – the theft of privileged credentials is the golden chalice of hacking. Here, a human factor, such as the [automated click response](https://www.metacompliance.com/blog/phishing-attacks-why-dont-we-think-before-we-click/), comes into play.

**Scan and Exploit – human failure:** hackers use anything that makes life easy and being able to automatically scan for vulnerabilities is a useful vector to malware infection. IT system components, such as web servers, databases and cloud apps, can end up misconfigured if the impact of poor security is not fully understood. Insecure apps and web components result in security holes that hackers can exploit. In this case, human failure leads to cyber security risk.

**Unauthorised use of credentials – human failure and human factors:** credential theft leads to unauthorised access to IT systems and resources. Ways that credentials can be used without authorisation include:

* **Shoulder surfing:** credentials are stolen when a malicious person watches someone enter a password.
* **Phishing**: tricking a person into entering login credentials into a spoof login page.
* **Social engineering:** tricking a person into handing over a login credential over the phone, social media, or using other communication methods, such as emails, help desks and texts.

In all three of the most successful hacking vectors, both the human factor and human failure loom large. Cyber security risk is concentrated in our employees and non-employees, but how can we reduce this risk?

**Best Practices Preventing Human Factors From Becoming Human Failures?**

A [study by Kaspersky](https://www.kaspersky.com/blog/the-human-factor-in-it-security/), which focused on the part that human factors play in cyber security risk, found that “careless or uninformed staff”” are the second most likely cause of a serious security breach; malware infection is the first, but is often itself caused by careless or uninformed staff. With high levels of risk associated with human factors, reducing failures is vital to mitigating security risk.

Two areas stand out that cover both careless and uninformed staff:

**Careless decisions That Lead to Security Failure**: making poor security choices, such as misconfiguring IT systems and components, or clicking on a phishing link before thinking, are human failures that lead to increased cyber security risk. Misconfiguration of IT systems and components is an example of a careless security decision. Clicking a phishing link is another. Both IT and non-IT staff are capable of careless decisions that lead to security failures. Ensuring that all staff, both technical and non-technical, are made aware of the impact of their choices, is a fundamental way to mitigate cyber security risk.

**Uninformed Staff Leading to Security Failure:** if staff are not aware of their actions, how can they possibly know the security consequences? Companies routinely train staff in other areas of the business, and this should be extended to security awareness training. Staff training in security includes an understanding of how phishing works, as well as other common security failures, such as password sharing and misdelivery of emails. Notably, misdelivery continues to climb as a form of human error according to the [Verizon Data Breach Investigation Report](https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf) (DBIR)