Picture credit: AdobeStock

THE INTRUDER WITHIN

Richard Hilson *explains why humans are the weakest link in your CNI security chain*

Security technology has witnessed huge advancements in recent years, particularly for those protecting critical assets or information. Facial and fingerprint recognition, ANPR and even 'mac addresses' or a person of interest's gait now all make up the technology toolbox of forward-thinking organisations' security policy.

However, humans remain the weakest link in any security chain, and the only way to correct this is to eliminate the human burden.

As with any workplace initiative, be it a simple recycling policy or a corporate password protection directive, technology is only as good as those who implement or operate it. While technology can be fallible and gremlins do arise, it's never as flawed as us mere humans with our unreliable 'on/off' switch.

Likewise, we carry the ability to reason, override procedures or ignore policy should we wish. Or as it happens, just make mistakes. In fact, according to a recent Verizon report, two out of three insider attacks happen as a result of negligence, and 74 percent of organisations are saying that insider threats are becoming more of a concern for them.

Employees who share access credentials risk unintentionally exposing them to unauthorised individuals

Richard Hilson is head of sales for security access management specialist Parking Facilities.

Security breaches aren't limited to external threats either, whether intentionally or not, they can come from within. Humans can, and do, 'go rogue', whether that's pre-meditated criminal or malicious intent or just by taking shortcuts.

And while data breaches court most news headlines in this digital era, some of the most significant security risks are those posed when employees neglect fundamental security practices such as sharing passwords or access cards.

Insider negligence remains one of the leading causes of security breaches. Employees who share passwords or access cards may do so out of convenience, ignorance, or a misplaced sense of trust. Unfortunately, this creates vulnerabilities that are left open to exploitation. When multiple employees share credentials, it becomes difficult to trace actions to a single individual. This lack of accountability can complicate incident investigations and allows malicious activities to go undetected.

Furthermore, the sharing of passwords or access cards means inaccurate accounting of personnel, and in the event of an evacuation or major incident, central IT systems will hold misleading information of employees' locations which could have a huge impact upon safety and potentially emergency services resources.

MALICIOUS INTENT

Employees with malicious intent can exploit shared credentials to carry out unauthorised activities while shifting blame to others, increasing the risk of deliberate sabotage or theft of sensitive data. Even when there is no malicious intent, employees who share access credentials risk unintentionally exposing them to unauthorised individuals, such as contractors, visitors or external attackers.

Access cards are designed to limit entry to restricted physical locations. When shared, unauthorised personnel can enter secure areas such as control rooms, rail lines, large construction sites, data centres, power plants or indeed any site meant to be kept secure. This creates opportunities for sabotage, theft or corporate espionage.

Likewise, shared passwords can lead to unauthorised entry into IT systems, allowing hackers to install malware, ransomware or spyware. For example, a cyber criminal gaining access to an energy grid system can shut down power to entire regions, causing chaos to millions of people and disrupting essential services.

And not all data breaches are caused by online hackers gaining entry through unsecure firewalls. Sensitive information held within critical sites, such as blueprints, system controls and customer records, becomes vulnerable when access credentials are shared too, and the disclosure of such information can have a serious impact upon a company's bottom line, operations and ultimately reputation.

One way to prevent human error, or to thwart malpractice is to reduce the burden upon employees to be compliant and eliminate our flaws by using technology that requires no intervention, decision-making or reason.

Facial recognition is widely used in the civil world now, despite the concerns of various lobbyists. Used correctly it is not a 'catch all', but an instant recognition of persons of interest cross referenced against a database of known suspects.

Our car parks are governed by automatic number plate recognition (ANPR) to gain access in and out, while border controls are using advanced biometrics for everything from facial and fingerprint recognition, through to recognition of human characteristics and gait, for both entry and to apprehend. The UK Home Office is even accelerating its transition to digital border management, using biometric technology to improve efficiencies, safety, and to track and capture known or illegal persons.

TWO OUT OF THREE INSIDER ATTACKS HAPPEN AS A RESULT OF NEGLIGENCE

But what of the corporate world? What of the CNI sites, airports, national construction developments such as HS2 or high-rise office spaces?

We always ask this very question, and also: "can you afford a security breach" in whatever environment you're in? Because the smart, cloud-based technology that are being used by governments, law enforcement authorities and Border Force have cascaded down through the civil and corporate worlds.

Security conscious organisations are now diligently removing human error, by eliminating the human burden. With cloud managed software not only are access points managed through biometric integration, but it also overcomes the issues mentioned earlier around accountability – in that the cloud will always register who has passed through an access point or out of it.

This is critical for both immediate safety and security, but also for matters arising from a crisis or emergency situation. It's also less admin heavy, more cost effective and can manage and store employee records, including background checks. Employee or contractor data is encrypted, information is safe, interactions are secure and businesses are protected.

Simple acts of negligence, such as sharing passwords or access cards, can open the door to catastrophic consequences, operational disruption, financial loss and even, in the case of CNI, national security risks. To mitigate this, organisations can do worse than to implement robust access management systems, and in doing so, release employees from having to be accountable for ensuring the security of the sites in which they work.

As artificial intelligence evolves, I see even more robust biometrics coming to the fore, until such time we work and live in environments that are controlled without us even knowing security checkpoints are all around us, and access management happening at every step. It will become as 'every day' as an automatic door allowing entry into our local supermarket, but we're not quite there yet ●