KCS Group International

We look at the world differently...

Cyber Security – who cares?

April 2025

In a world where headlines constantly report rising inflation, new taxes, and perplexing government policies, it's no wonder that massive cyber-attacks, resulting in the theft of millions of pounds and countless personal data, often go unnoticed.

Many people assume these attacks are orchestrated by state actors such as China, Russia, Ukraine, North Korea, Iran and even Pakistan, leading to a fatalistic belief that there's little they can do about it, especially if even IT security experts struggle to combat such threats. The general attitude is often "*It doesn't affect me".*

However, the reality is more complex. State actors do, indeed, engage in cyber warfare, collaborating with organised crime groups (OCGs) to exploit vulnerabilities in IT systems worldwide. While many of us may not work in government or critical infrastructure sectors directly targeted by these attacks, we are all part of organisations that are equally at risk, often at the hands of local gangs and individual hackers.

The media frequently assure us that large corporations have "*robust security teams*" equipped with the resources needed to tackle these threats. Yet, in times of economic strain, cybersecurity is often one of the first areas to face budget cuts. This trend leaves many organisations vulnerable to attacks.

Weaknesses in IT Security

IT departments face significant weaknesses that compromise their security.

• Updates

Keeping systems up to date is a monumental task. It's not just about core company systems; every terminal must receive updates for all software, including specialised applications used in specific departments.

• Patching

When vulnerabilities are discovered, it's crucial to patch them swiftly. However, the time between identifying an exploit and developing a fix can leave organisations exposed. Often, companies only recognise a new threat after they have already been compromised.

• Human Error

The most significant vulnerability lies with the users themselves. Cybercriminals exploit human behaviour, and the desensitisation to cyber threats is a major concern. Without realising it, employees can become unwitting accomplices in cybercrime and become complacent.

• The Human Factor

Neglecting cybersecurity is detrimental not only to your employer but also to you personally. Many employees overlook basic security practices, such as changing their passwords regularly or securing them properly. Some still even leave passwords written down in plain sight, akin to leaving their house keys on the doorstep.

• Cleaning Staff

Often, cleaning staff are external contractors with little loyalty to the company. They may not think twice about taking sticky notes with passwords on them and handing them over to someone outside. Just because you believe your information isn't valuable, it doesn't mean it isn't. Your data could lead to more sensitive information within the organisation. The incidents of cleaning staff being actively involved, indeed participating in a hack, are legend.

• Employees and Social Engineering

In a world where financial pressures are mounting, the allure of a "*freebie*" can be irresistible. There have been instances where OCGs deliberately drop USB sticks in a company car park or in reception, anticipating that a curious employee will plug it into their computer. This is not new, but this innocent act is still being committed and can grant cybercriminals unwarranted access to corporate IT systems, compromising not just the organisations data, but also the employee's personal information.

• Consequences of Negligence

A recent IT survey revealed startling statistics: nearly 50% of cyber breach events involved individuals who had received formal warnings or disciplinary action. In 27% of cases, the employee was fired, with financial institutions being particularly stringent, firing 31% of offending employees.

Conclusion

Cybercrime is not merely a distant concern; it's a pressing issue that affects everyone. Apathy towards cybersecurity can have serious repercussions, not just for your employer, but for your own career and security.

In today's digital landscape, especially with the increase of hybrid warfare courtesy of our friends from overseas, we cannot afford to be lax or complacent. Receiving a formal warning or losing your job over a seemingly minor mistake is a reality many people may face.

So, who cares? You should - because cybercrime is everyone's problem, and awareness is the first step towards protection.