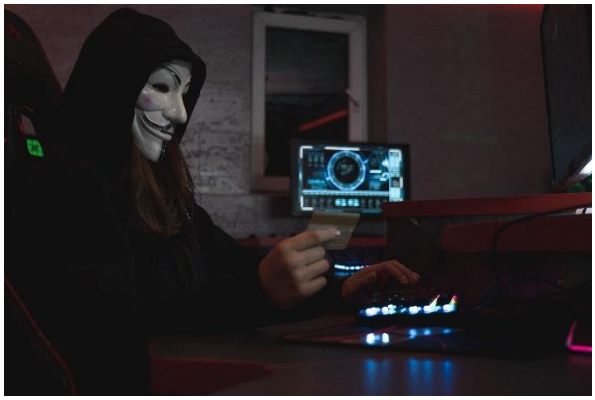
KCS Group Europe

Cyber Security in the Workplace

October 2022

IT vs Cybersecurity: Not where the battle lies



Information technology (IT) is concerned with the storage and transmission of digital information. Cyber-security is the protection of the same: both the information, and the means by which it is stored or transmitted. It is crucial that the two are never seen as 'at odds' with each other but rather as complementary. Vital, also, that cyber-security is accepted as the responsibility of the entire organisation and not as a purely 'IT' issue. Not only does a technology-driven approach to cybersecurity overlook critical human elements and failings that, with proper education, can be addressed, but hiving off a business-critical issue to one department alone can foster conditions of arrogance and ignorance at senior levels which have a negative effect on all levels and departments of the company.

Human error

Whether as a response to a security-driven restriction, an attempt to make their own job easier, or simply because nobody told them not to, employees are adept at finding ways to bypass security measures or unwittingly expose their organisation to significant risk. In part, this may come from daily practice, for instance discarding rather than shredding documents (both physically and digitally), automatically saving passwords, or leaving them stuck to the monitor, or assuming that if an individual, file or device is in the building, then it has a right to be there and leaving it at that. ('Low-tech' intrusion attempts whereby pendrives are mysteriously left lying around the office waiting to be plugged in, or an individual with a suitable namebadge or uniform is left to their own devices, do not even require the cyber-department to prevent them). However, there are a variety of more dedicated schemes that rely not only on human error, but the errors embedded in organisational process that do not counter or prevent these.

Phishing

Whether by email, telephone or text, a phishing scams sees an individual lured into providing sensitive data (personal identifiers, credit card details, passwords and so on) on the false assumption that they are being asked to do so by a legitimate institution.

Identity theft and financial damage can then ensue. Quite apart from the ways in which the intended victim should be able to spot the scam – bad spelling/grammar, a misspelt domain, an out-of-practice request such as the presentation of entirely new banking details, or a file type that does not match the reality – it is the responsibility of the company management to enforce measures of scepticism, to say that no suspicious email or file is opened without quarantining by the IT department beforehand, or no transfers are to be made without making direct return contact to the client/customer and double-checking. While the IT department can facilitate departmental risk avoidance, the pressure to call upon them must come from the top in a synergy of having the help on hand and knowing when to use it.

The most common variant of phishing affecting corporates is that of Business Email Compromise (BEC), whereby emails claiming to be from a known party compel the recipient to actually engage with, or transfer money and information to, bad actors. For instance, in 2016, the Belgian Crelan Bank lost $75.8m USD as a result of criminals presenting themselves as high-level executives and pressuring low-level employees to perform urgent tasks of money transfer. They even obtained the CEO's signature and stamp in order to lend credibility to their transfer request.

Ransomware

A form of malware, ransomware encrypts files on a victim's computer and the bad actor then demands payment – usually in cryptocurrency – in order for this data to be unlocked or returned. Infection can occur through multiple vectors: phishing spam (an email or attachment containing the virus that, once opened, infects the entire network), exploitation of pre-existing security gaps to secure administrative access, or 'under cover' of a different form of cyber-attack so as to distract attention from the bad actors' true objective. But regardless, ransomware can be devastating for a company with neither the policies and defences to prevent it, nor a backup of their data.

A ransomware attack is a highly coordinated team effort that can take months of preparation with the sole intention of disrupting a specific business and extorting a payment. Just the amounts requested are varied from a few hundred dollars to a few million, so too do targets range from small businesses (perceived, rightly, or wrongly, as being less secure) to major government and international institutions.

Essentially, everyone is at risk. And if the ransom is paid, business cannot return to normal: not only will there be the spectre of another attack on the basis that if you paid once, you are likely to pay again (if indeed your data is even returned), but the financial (insurance, legal fees) and reputation (business disruption, client criticism) costs can be immense – if not fatal.

False narratives about ransomware also need to be countered. Military-grade encryption is used in ransomware attacks, and not even supercomputers can decrypt this in a suitable time frame. Organisational IT engineers will have no chance. Once the data is gone, it is gone. Multiple devices are infected as ransomware spreads laterally across a network, with dormant code often being laid down before in the aforementioned 'distraction' attacks so as to ensure full coverage. And as previously stated, hackers – not the most ethical individuals – are under no inducement to return your data at all. Traditional firewalls and antivirus perimeter defences are not adequate to protect against the modern ransomware attack. Multiple layers of proactive protection are the absolute minimum.

Targeting data

It is a reality that organisations of all sizes and types are becoming victims every day, and they are all at risk. It is possible for small businesses to be victimized by ransomware and be extorted by exposing employee information, client lists and credit card information, just as it is possible for multinational conglomerates or even governments to see the most sensitive data be stolen or ransomed. Criminal gangs and ransomware variants show no signs of slowing down with cyber-experts predicting that damages will exceed $30bn USD worldwide in 2023, taking advantage of the ongoing lack of joined-up thinking and synergy, and pre-existing gaps.

Crucially, the threat portfolio is broadening, not only in the source of the activity and its methodology, but its motivations. State-sponsored bad actors now account for a good deal of the activity, and these are far better resourced and more dangerous than the traditional 'lone wolf' criminal. And where states are concerned, money is not always the primary target: information is, and any access into an organisation either for its own merits or as a step up the chain is not one that will be passed up.

While the two-year Covid period saw an upswing in ransomware and phishing for financial gain, as a result of remote working and decentralisation of IT security, the current global destabilisation caused by the war in Ukraine is seeing Russian- and Chinese-led efforts to disrupt and destabilise the West on a more general economic and informational footing.

While Austria and Spain of the Western European nations seem to be bearing the brunt thus far – Austria because of a well-established Russian presence from Vienna outwards during the Cold War, and old habits dying hard, and Spain due to its perception as the 'soft underbelly' of Europe as far as cyber-security is concerned – it has, however been said in certain quarters that numerous organisations have gone out of their way to conceal the true scale and extent of breach attempts in the UK so as to keep concern and public alarm to a minimum. The best attitude is to assume that you are being targeted and act accordingly: not only investing in cyber-security from a financial perspective but ensuring that a security culture is predominant across all aspects of the company.

KCSGE provides proactive cyber services targeted at preventing and mitigating cyber-attacks. Our cyber service catalogue includes: