ENJOY SAFER TECHNOLOGY™

CYBERCHOLOGY: THE HUMAN FACTOR

INTRODUCTION

Every organisation is now a digital business. Driven by developments in technology, companies have digitised their services and offerings to meet the ever-growing demand from consumers. However, evolution also comes with its own risk, and in this case, it is a significant rise in cybercrime that is extremely diverse and unpredictable.

Despite the risks involved, cyber security is something many businesses leave up to dedicated IT specialists, when in fact a lot of breaches could be avoided if a more integrated and business-wide approach to cyber security were adopted.

This paper, compiled in partnership with ESET, a global leader in IT security, and The Myers-Briggs Company, the business psychology organisation, investigates the link between personality type and vulnerabilities to cybercrime.

CYBERCHOLOGY: **THE HUMAN FACTOR**

Data is the new gold, and criminals everywhere are panning for it. So, it is vital that modern businesses have a degree of self-awareness regarding cyber security. That is, not just a general awareness of the problem, but a detailed and personalised knowledge of how cybercrime and cyber security relate to their own operations.

A survey conducted by ESET reveals that 42% of businesses are focusing on delivering compliance training as part of their cyber security protocol, while over 63% use passwords as a gate keeper of their systems. Yet human error is a major factor in many cyber breaches. There is often a lack of team coherence regarding cyber security, despite the fact that every team member in a modern business will have access to and be using vulnerable systems on a regular basis. Cyber security is something which too many businesses leave up to dedicated IT specialists, when in fact a lot of breaches could be avoided if a more integrative and business-wide approach to cyber security were adopted.

The conversation about cyber security needs to be happening in the boardroom and teams across the organisation. For the human risk factor to be mitigated, both senior and middle management need to play a much larger role in both identifying vulnerabilities within their teams and securing cyber systems via an integrative human/machine approach.

THE PROBLEM

Cybercrime is common and pervasive. Every business can expect to experience a cyberattack at one point or another. What makes it so difficult to combat is the fact that cybercrime is also a nebulous thing. It is impossible to predict when a cyber-attack will come, what the motivation behind it will be, or even who the perpetrator will be. For example, a teenager from Leicestershire hacked the Pentagon for no reason other than to prove that he could do it. Hackers and cybercriminals can be anyone, anywhere, and their modus operandi are extremely diverse.

There is a large variety of strategies that can be employed by cybercriminals.
Some of the biggest trends we are currently seeing include:

- **Formjacking.** Formjacking codes, as the name suggests, target online forms. Typically, a formjacking attack will skim credit card details as they're entered by customers of online retail sites.
- **PowerShell.** PowerShell, or 'Living off the Land' attacks rely on eccentric behaviour in order to feed off supply chains. A PowerShell script will disguise itself within a 'safe' process (the 'shell') and phish for data and/or intelligence from therein.
- **IoT Attacks.** The Internet of Things provides a plethora of opportunities for cybercriminals. The need to secure smart devices (for example, an Alexa-enabled speaker) against cyber-attack is often overlooked, making these an easy portal via which cybercriminals can access a system.

SYSTEM VULNERABILITY AND HUMAN ERROR

Cybercriminals are not constrained by the same restrictions which govern legitimate software developers and white-hat hackers. This enables cybercriminals to implement changes at an unprecedented speed, enabled by ever evolving technology including Artificial Intelligence. For example, ransomware (software which takes control of systems and/or data and hold it to ransom) has recently been supplanted by more direct methods of skimming cash or stealing data to sell on. This change happened even before white-hat developers had got to grips with ransomware. Time after time we've seen that the next 'Big Thing' in cybercrime goes live before we've even started getting to grips with the last Big Thing. So, while the trends mentioned above may be dominating at the time of writing, the MO of any cyber criminal worth their salt can and will change in a number of unpredictable ways, and will do so extremely quickly.

However, what is notable about the most successful cyberattacks is that they rely on a degree of human error and/or ignorance. For example, cybercriminals are able to install phishing codes onto systems via Alexa because many people are unaware of the need to protect their smart devices as well as their desktop computers. In a business context, there is often a lack of awareness about the need for a truly integrative and self-aware approach to cyber security, one which encompasses everyone and not just the 'boffins' in the IT department.

WHY IS THIS IMPORTANT?

Many people still have an old-fashioned view of cybercrime as something done for fun by malcontents. According to this mindset, the unwary may end up with a file-garbling virus but, overall, it's more annoying than it is seriously damaging.

In fact, cybercrime is a lot more insidious and far wider in impact than this. Modern cybercrime has become a multi-trillion-dollar industry. Here are just a few of the potential impacts which can result from a cyber security breach:

- **Financial losses.** Whether it's as simple as losses resulting from downtime or as complex as ransoms and/or fines, serious cyberattacks always have an immediate monetary impact.
- **Brand damage.** Even if you manage to neutralise the threat and clean out your systems, your brand is still likely to suffer as a result of a cyber security breach. In the wake of scandals like Cambridge Analytica, consumers are very wary of their data. They need to trust brands before handing over any details – and a cyber security breach makes a company unworthy of that trust. Major loss of custom follows on naturally from brand damage.
- **Legal penalties.** The GDPR and other regulations take data protection very seriously. If a cyberattack results in a data breach, your business could well be found liable for not taking adequate data protection measures. Fines and penalties for this are heavy.

THE HUMAN ELEMENT

Given both the serious repercussions of cybercrime and the key role that human error plays in cyber security breaches, it is vital that a more holistic approach is taken to cyber security.

ESET and The Myers-Briggs Company advocate an integrative human and machine approach, which recognises the strengths and weaknesses of both human team members and the digital systems they're working with. Using psychometric tests to build self-awareness can play a big part in this, as can multi-level training. Individuals and their managers (rather than IT departments and outside contractors) are the truly key players where cyber-security is concerned.

Research collated by The Myers-Briggs Company that looked at individuals across Europe shows that different kinds of cyber security errors are more common among people with certain personality preferences:

- People with more Extraverted personality types (those that work out ideas by talking them through) tend to be more vulnerable to manipulation, deceit, and persuasion from cybercriminals. These kinds of attacks are known as 'social engineering' attacks, and they're particularly effective against Extraverted types (who may be more susceptible to social overtures). However, being highly tuned towards external communication does work in Extraverts' favour in other situations – Extraverted people are generally faster to pick up on attacks coming in from outside.
- People with a preference for Sensing (those that observe and remember details) are more likely to spot phishing attacks than their Intuitive counterparts. However, those that have the preference for Sensing are also more likely to take cyber security risks, particularly when they also have a preference for Perceiving (those that are more flexible and casual) and/or Extraversion (those who are sociable and are expressive).
- People with a preference for Feeling (those guided by personal values) and people with a preference for Judging (those who are systematic or structured) are more likely to fall victim to social engineering attacks than those with a preference for Thinking (those who solve problems with logic). However, people who have the preference for Thinking can over-estimate their own competence, leading to mistakes, whereas Judgers and Feelers tend to be more cautious and therefore more rigorous when following cyber security policies.

So, all personality types have different strengths and blindspots that can impact the outcome of a cybersecurity attack. Identifying where these lie and how they might correspond to your cyber security protocols is a great first step in building a coherent, integrative cyber security programme. For example, people with a preference for Intuition (the opposite to Sensing) will really benefit from being reminded to look at the detail of emails – does the sender's address look odd for example (something they are less likely to do naturally).

Those with a Thinking preference can be encouraged to see a correct approach to cybersecurity as an expression of their own competence. Building an individual's self-awareness will help them to take responsibility for their own cybersecurity. Overlaying organisation-wide self-awareness with a robust cyber security system can create a net of human/digital skills and proclivities which cybercriminals will have trouble slipping through.