

DEFENCE!

IT IS ALMOST IMPOSSIBLE TO PREVENT A CYBER ATTACK, BUT THERE ARE STEPS THAT FIRMS CAN TAKE TO ENSURE THEY UNDERSTAND THE THREATS AND PUT MEASURES IN PLACE TO DEFEND AGAINST ATTACKS. THESE STEPS SHOULD COVER...



CONFIDENTIALITY which is about ensuring the protection of data by preventing it from getting into the wrong hands.



INTEGRITY which comprises the accuracy, trustworthiness and validity of information. In other words, the processes and procedures that need to be in place to prevent changes to data, either in error or on purpose.



AVAILABILITY as information must be accessible to authorised personnel whatever the circumstances, an incident response plan must be in place to ensure operational continuity, should the worst happen and a firm's systems are breached.



PEOPLE who are typically the weakest links, must be aware of their role in preventing and reducing cyber threats. Effective cyber security training can help reduce the risk of cyber threats aimed at exploiting people.



PEOPLE are also your first line of defence, so board members, supported by specialised technical cybersecurity staff, need to be aware of cyber security risks and of the plans in place to mitigate their impact. Cyber security staff need to keep up to date as those who don't affect a firm's ability to respond to and defend against attacks.



PROCESSES AND PROCEDURES are crucial in defining how a firm's activities, roles and documentation are used to mitigate cyber risks. Cyber threats change constantly so processes and procedures need to be adaptable and continually reviewed.



TECHNOLOGY is the means to cyber security breaches, but it is also a potential solution to them. Once a firm identifies the risks it faces, it can put in place the technologies to mitigate threats.

Authentication is the process by which a system confirms that a person trying to access it is allowed to do so. Most systems rely on a combination of one or more of the following elements:

- » A thing you know.
- » A thing you have.
- » A physical attribute (e.g. fingerprint).

SINGLE-FACTOR AUTHENTICATION (1FA) is probably the way you log into your computer at work, combining, for example, a user ID and a password (two things you know).

TWO-FACTOR AUTHENTICATION (2FA) is becoming more common in the workplace and will use a thing you know (a user ID and password) and a thing you have (a remote key that generates a unique code) or a thing about you (a fingerprint). Getting cash from an ATM, which requires a PIN (the thing you know) and a card (the thing you have) is an example of 2FA.

THREE-FACTOR AUTHENTICATION (3FA) uses all three elements, for example, an ID and password (the thing you know) and a unique physical key (a USB stick – a thing you have) with a fingerprint scanner (to verify the physical attribute).

