Two hundred and fifty years since the forces set in motion by the Industrial Age were unleashed, some of the effects, such as global warming, are only now beginning to be understood. After only 30 years, the Information Age is already profoundly changing all aspects of life and will continue to do so. Advanced electronic equipment and fast, cheap communications mean that many previously static aspects of daily life, including physical security, are lagging behind the new reality that has been created.

In the days before the Internet created a global information-sharing network, ‘security through obscurity’ was a more viable strategy. Now, those with criminal intent can go from zero to dangerous in 60 minutes by searching the Internet for a tutorial. The threat is not just from malware or hackers; physical security mechanisms are also at risk. From videos of how to open cars with a tennis ball to sites dedicated to opening so-called ‘high-security’ locks in seconds, key areas of the physical security environment may not be as secure as one would think.

Inscribed on the Temple of Apollo at Delphi (Greece) was the imperative to ‘know thyself’. Organisations wishing to tackle the challenges of the future would do well to start from a position of self-awareness. One of the causes of the ‘credit crunch’ was that banks and regulators did not really understand the level of risk that they faced. Likewise, security officers need to understand the vulnerabilities, limitations and dependencies of information systems in order to successfully mitigate risks. While many organisations are getting better at identifying and understanding digital weaknesses, the inherent weaknesses of physical devices are not as well recognised. Certainly, uncontrolled physical access to computers can be devastating—a so-called ‘evil maid’ attack can cause the compromise of sensitive information.

In 2007, the German magazine Der Spiegel reported that Mossad agents broke into the London hotel room of a visiting Syrian official and planted malware on his laptop. According to the magazine, information gleaned by the malware was used to degrade Syrian air defences in a bombing raid on an alleged nuclear facility. Even if an enterprise does not have a national air defence system to protect, it is worth understanding the limitations of its physical security devices because if the enterprise does not, its attackers more than likely will.

In February 2011, UK customers of Vodafone (a mobile telephone company) experienced problems accessing voice, text and mobile Internet services because of the theft of network equipment and IT hardware from a data centre that was broken into in the middle of the night.

Just as computer hackers try to make systems perform in ways in which they are not supposed to, lock pickers try to do the same to a lock, i.e., by making it allow access to someone who does not have the correct key. For too long, lock-and-key security has been based on ‘security through obscurity’, with knowledge and tools carefully protected by locksmiths. However, the Internet has burst the obscurity bubble as thousands of people share information about weaknesses and bypasses for particular locks. Specialist tools are now available at high street prices and can be possessed in most countries without legal sanction. Why risk noisily jimmying a lock now that there are scores of web sites and videos dedicated to lock picking and lock ‘bumping’, which can help a person silently open a door in seconds? (Typing the name of a specific door lock and the ‘bump key’ [available for around US $10 plus shipping and handling] into a search engine is not for the faint-hearted.)

Researchers at the University of California, San Diego, USA, using off-the-shelf equipment and software, recently photographed a key from 200 feet above and successfully made a copy of it. By proving that keys can be photographed from a distance and accurately copied, the researchers have undermined old assumptions about physical keys being ‘secret’.

Peter English, CISM, is corporate risk advisor for a local government in Scotland.
It is, however, important not to focus too much on locks and doors because criminals are well practised at defying threat models. In response to car immobilizers, thieves started breaking into houses to steal the keys; a prolific burglar who was recently jailed in the UK defeated home security measures by removing tiles and then cutting his way in through roofs.4 The less-imaginative crook could always use the tried-and-tested technique of smashing a hole in the drywall or a window.

Many security officers will be aware of certifications such as the Common Criteria and accompanying Evaluation Assurance Levels and will choose their equipment accordingly,5 but, often, physical security items are purchased by another department without information security being considered. Physical security standards also exist. For example, in the UK, the Loss Prevention Certification Board (a collaboration amongst government, manufacturers and the insurance industry) tests the security claims of products to destruction according to Loss Prevention Standard 1175.6 The standard’s security levels range from 1 to 8—with a product security rated as 1 resisting entry for one minute to opportunistic attacks using limited tools up to a product security rated as 8, which is certified to resist entry for 20 minutes from professional attackers using extreme means with a wide range of tools (including electrically powered tools such as saws and drills).

Just as security officers would want to know exactly what a vendor means when it reports that a product is ‘secure’, so should physical security claims be queried and tested. Penetration testing physical security by seeing how much effort it requires to defeat a door or window is unlikely to be popular at any business, so using products based on the correct certification standards for one’s country is important. A physical security asset that is certified to withstand, for example, 10 minutes of attack allows more accurate incident-response plans to be developed, such as reducing the gap between a break-in being detected and the time it takes for key holders or law enforcement to travel to the scene. Furthermore, certification standards help provide reasonable assurance to the organisation that its information assets are properly protected and allow some quantification of the organisation’s ability to withstand an attack.

Depending on the severity of the threat environment faced, the UK government’s information risk assessment guidance (Information Assurance Standard 1) refers to three levels of preparedness for computer systems: aware, detect and resist, and defend.7 This categorisation could equally apply to physical security. At a minimum, security officers should be aware of the limitations of physical security (i.e., as the ancient Greeks advised, they should ‘know themselves’) and perhaps move sensitive assets to a different location or put in place compensating controls. Where sensitive assets are at risk, measures that will detect and resist attacks, i.e., those that are tamper-evident or alarmed, should be deployed. Finally, where assets are mission-critical, physical security measures that will defend those assets from unauthorised access for a certified level of time should be put in place.

Security officers are perpetually in a race with well-motivated threat actors, which is why layered security controls are important, but the profession tends to focus on the technical challenges to the detriment of the physical and, hence, overall security levels. No security officers worth their salaries would say ‘the enterprise is fine because it has a firewall’, and no security officers should be satisfied with the words ‘that building is secure because it is kept locked’.

ENDNOTES

5 Common Criteria, www.commoncriteriaportal.org