

Let's get physical

Physical access security is an oft-neglected aspect of information security, writes Kevin Fitzgerald.



When two men walked into the security-protected Australian Customs Service at Sydney's International Airport in late August this year and wheeled two computers allegedly storing Top Secret information past the security guards, we asked: 'How come?'

It's all a matter of how you 'sell the dummy' or exploit human social engineering. If you wear the correct attire, in this case that of computer technicians, security may just allow you to gain entry.

It helps if you sign on as current employees. But to do something as audaciously breathtaking as actually wheeling out two computers on a trolley, why wouldn't you be stopped? It's a good bet that the security operator had not seen such activity before. He probably thought they were carrying out special maintenance procedures.

What is wrong here?

First, security levels must be established to reflect the

sensitivity of the information stored. Is the work environment classified as Public space, as Proprietary space, Restricted space, or is it Secret space, even Top Secret? Such levels define the security levels of the work environment and all may be present within the one building.

If the work space is a Top Secret site it requires Top Secret security levels. Evidently this had not been done in the work environment at Sydney Airport. If it had, a formal information security policy would have set the framework around which security was built. Part of this policy would have addressed physical access security. It would have insisted that at least double-factor authentication be used to gain entrance, no matter who was attempting access. An example of authentication that would have prevented this incident is the use of pre-registered signatures and photographs for each named person allowed entrance. Sometimes such photographs and signatures are held

on swipe cards to provide a third layer of authentication.

By simply allowing a name and signature to have access without checking pre-registered versions is a clear indication that security practices are slack and awaiting challenges — the Sydney attackers had done their homework.

Second, security staff must be trained to take security seriously. This follows from a security culture that pervades the organisation and acts as a strong deterrent to would-be attackers who quickly identify soft targets.

There must be no exceptions in organisations with the need for high levels of security. Kerry Packer, it has been said, quickly created an access security culture in his time at Channel Nine by sacking the car park guard when he recognised Packer's car and waved him through without checking his credentials.

Third, employees, both permanent and part-time, as well as contractors must have their special situations recognised. Those who are not full-time must only be allowed on-site when they are expected unless they are supervised at all times — sometimes a difficult task. All types of employee must go through some type of 'exit' procedure when they finish working at the site. In high-security areas, not only access but also egress should be controlled. In security circles we often hear of visitors stowing away for a few hours and joining the late-night cleaning staff to carry out an attack.

A work environment that is rich in sensitive information must enforce a clean-desk policy. Not only papers but also disks and computers must be locked away, especially laptops and other portables. Sensitive waste paper must be shredded, not given to the local kindergarten as has actually happened.

Access security hardware such as closed-circuit TV, door

'In high-security areas, not only access but also egress needs to be controlled.'

barriers, swipe cards, perimeter alarms, authentication devices, vaults, and locked cupboards are all part of the access security armoury. However, even with all of these things in place persons in the correct 'uniform' bearing access cards, false names and forged signatures can still get in and out. What will stop them in their tracks is a security-aware workforce.

Apart from the guards in the entry hall, the office staff, the warehouse staff and the factory staff all have significant security roles. If they lock up the sensitive areas and the sensitive materials, if they are aware of strangers in areas they should not be, if they refuse to allow entry to someone who is not known to them but who appears confident, or even who is known but does not have the correct access keys, they will define the organisation as security-aware. It will not be a 'soft option'.

Such an organisation will not lose two valuable computers holding sensitive information that acutely embarrasses the government. And in this type of organisation, Packer would have to roll down his tinted window even on the coldest of nights and show his pass just like everyone else. No doubt he would smile with the satisfaction that his staff was looking after the shop properly. □

KEVIN FITZGERALD
is an information security consultant with more than 25 years experience in designing and executing security solutions for large organisations.

