HOLISTIC SECURITY PROTOCOL

Douglas Miorandi *highlights the importance of pairing physical security with cyber security to protect data from all types of attacks*

Edward Snowden's name entered the cultural lexicon in 2013, after he leaked thousands of classified National Security Agency documents to journalists. He's been variously called a traitor, a patriot, a revolutionary, a dissident and a whistleblower, but however you feel about him, there's one way to categorise him that no one can dispute: he's a thief.

There's no doubt about it: Snowden's information didn't belong to him, and the scary truth is that he is neither the first nor the last employee to attempt to smuggle secrets out of a building – and we need to learn from his success to try to prevent it from happening again.

Since the dawn of the digital age, we've fought cyber pirates with tools like firewalls, encryption, strong passwords, antivirus software and white-hat hackers. But with so much attention on protecting against cyber risks, we sometimes forget about the other side of the coin: the risk that data will be physically removed from the building.

> MANY PROBLEMS CAN BE AVOIDED BY SIMPLY USING THE RIGHT TECHNOLOGY TO DETECT DEVICES

There are four main risks to physical data security – some of which you might not be thinking about, but all of which are imperative when creating a comprehensive approach to protecting critical assets.

THE INSIDER THREAT

Every company or government agency has at least one disgruntled employee working for them, whether they know it or not, and that means that every organisation is at risk of having data walk out the building with that individual at some stage.

People steal data from their workplaces because they see some means to an end, whether it's to expose something embarrassing or damaging due to a personal vendetta or because they can sell it to a competitor or the media and benefit financially – meaning they don't even need to be disgruntled; they might just want a way to make a quick buck. This can happen to both private companies as well as government agencies – don't forget that Snowden was a contractor working for the NSA. Financial data, too, can seem attractive, both for insider trading as well as to sell to the competition.

THE OUTSIDER THREAT

In addition to worrying about their own employees, companies and government agencies need to be wary of threats from outsiders. These can come in the form of the corporate spy – someone specifically hired to pose as a legitimate employee or private contractor in order to extract information – or the opportunistic thief – a contractor hired to work on a server or in sensitive areas who sees an opening and seizes it. Either one is equally damaging to sensitive data because of the physical access they have.

THE SEEMINGLY INNOCENT PERSONAL ITEM

There are two types of personal items that can be used to steal data: the commercially available off-the-shelf (COTS) variety, and the intentionally disguised variety. COTS devices include SD cards, external hard drives, audio recorders and even cell/smartphones, any of which can be used to transport audio, video and computer data in and out of a building. Intentionally disguised devices are straight out of the spy novel; they could be a recording device that looks like a car key fob or a coffee mug with a USB drive hidden in a false bottom.

The difference between COTS and disguised devices is that if one gets caught with a COTS device, security will know what it is and can confiscate it. The disguised device looks like a security-approved item anyone could be carrying into the workplace, making it especially devious.

Additionally, sometimes these devices don't just function to bring information out of a building; they instead are used to damage a server or hard drive once it's plugged in to a computer or the network. Some are both – a recording device that extracts data and then destroys a hard drive.

SCREENING

This risk creates or amplifies all of the other three. Whether it's an employee, an outside contractor or a device, the physical security risks are real and everyone and everything entering and leaving a building needs to be screened.

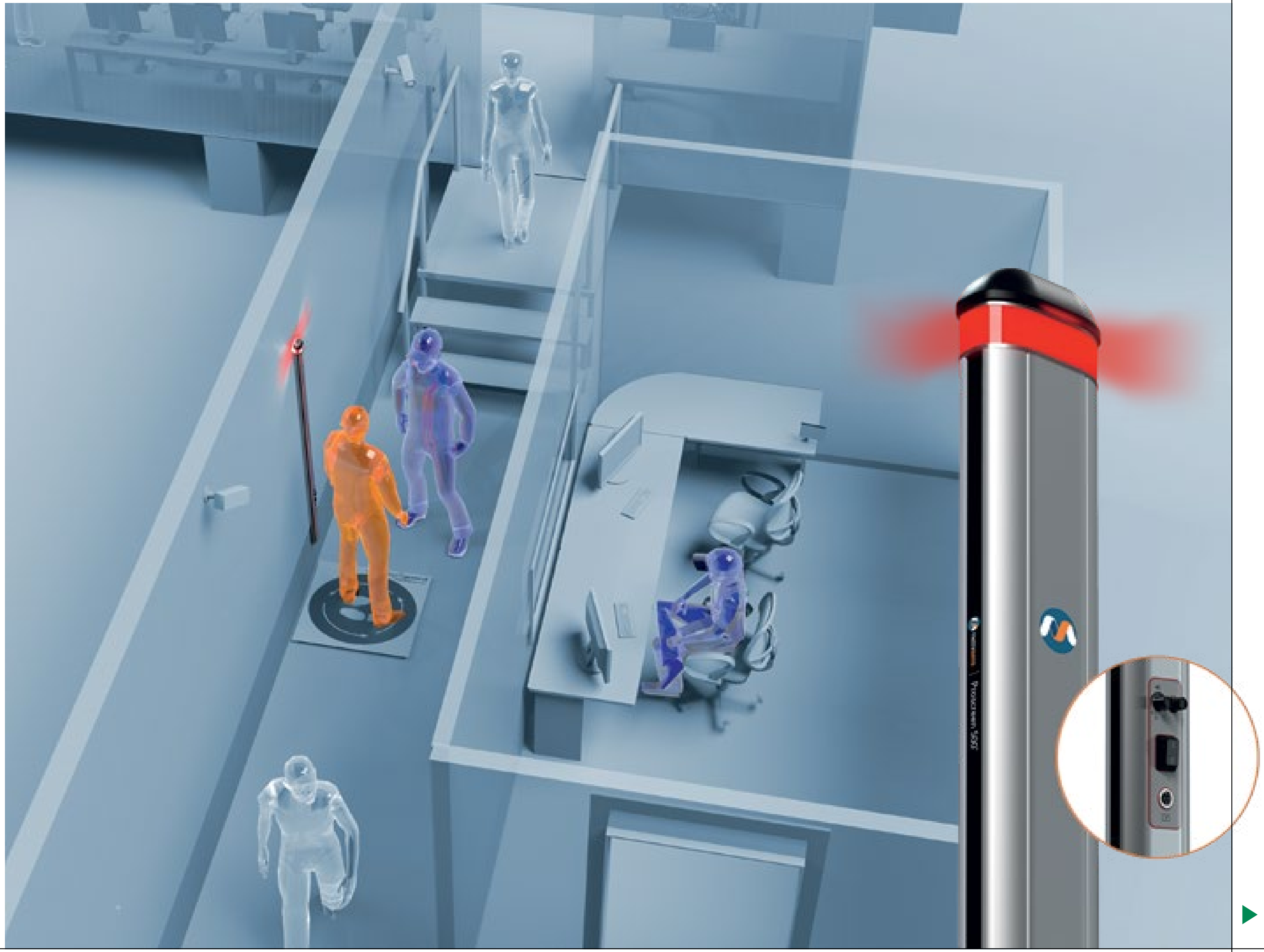
Unfortunately, screening often either isn't occurring at all or is ineffective or inconsistent when it does. Even companies with airtight cyber security protocols can sometimes fall down when it comes to physically screening people and stopping them from taking data on recording mediums.

This is a huge mistake, and the consequences can be dire. They range from loss of customer trust, exorbitant lawsuits and tanking stock prices in the private sector, to risks to national security in the public sector. Costs and resource use increase as well during efforts to reactively fix or mitigate the effects of physically stolen data.

For both sectors, the risk has never been greater that information will be physically removed from a building on a piece of hardware. Years ago, it was much harder for the average Joe to figure out where they could sell stolen data. Now, with the Deep Web, anyone with Tor can access forums requesting specific information from competing spy agencies, with instructions on how to deliver it, greatly reducing the risk of getting caught – and increasing the likelihood people will try it. Although it's getting easier to sell data, the good news is that all of these threats are avoidable with the right measures.

There are a number of ways to protect against these risks, and the first one requires a change of mindset. Not long ago, the building/physical security department and the IT/cyber security department were considered two different entities within an organisation, with little overlap or communication.

Organisations are now realising that, because of



FMDS can be used to find concealed objects including weapons or recording devices

Picture credit: Metrasens

▶

the level of risk they face from both internal and external threats, they must take a holistic approach to data security. Physical data security and cyber security must be considered the yin and yang of an airtight policy that effectively protects sensitive or confidential assets from a malicious attack.

Combining strengths will amplify results. For example, physical security managers can advise the cyber security managers on ways to reinforce their protocols – perhaps by implementing the newest surveillance cameras in sensitive areas or removing ports on servers so that external drives cannot be used. In turn, the cyber security team can let the physical security team know that they have outside contractors coming in to work on the server, and the physical security team can then escort the contractors in and stand guard as they work.

Constant communication and a symbiotic relationship between the two departments are the keys to creating an effective holistic security protocol – and once you've got the momentum going, don't let it slow down. Sometimes efforts start off strong and then peter out if priorities change, and when guards are down, it's an excellent time for a malicious actor to strike. Create an effective program, and ensure it stays effective and looks effective so people know it's not worth the hassle to try. It's not just about the mentality, though. Using the right technology is just as key.

CHOOSING THE RIGHT TECH

Because protecting the physical security of data entails a physical approach, many problems can be avoided by simply using the right technology to detect devices that can bring threats in and carry proprietary information out. Electronics such as hard drives, cellphones, smart watches, SD cards and recording devices have a magnetic signature because of the ferrous metals inside them. Using a ferromagnetic detection system (FMDS) as people enter and exit a building or restricted area means that anything down to a small microSD card triggers an alert, allowing confiscation or further action as needed.

In the most basic terms, FMDS uses passive sensors that evaluate disturbances in the earth's magnetic field made by something magnetic moving through its detection zone. Nothing can be used to shield the threat, because FMDS doesn't detect metallic mass; it detects the magnetic signature, down to a millionth of the earth's magnetic field.

Although it is a passive technology, it is more effective and reliable than using hand wands or the walk-through metal detectors typically seen in an airport, which cannot detect very small ferrous metal objects. FMDS can see through body tissue and liquids, so items cannot be concealed anywhere on a person or with their belongings.

Whether or not the items are turned on doesn't matter; FMDS doesn't work by detecting a signal, but rather by spotting the magnetic signature that electronics contain. This is ideal, because most recording devices do not emit any signal whatsoever.

This also comes in handy in the case of seemingly innocent items that contain recording devices. Someone coming through a walk-through metal detector with a small recording device concealed in a non-metal enclosure may not set off the detector, because there is such a small amount of metal in the device, but FMDS is sensitive enough to pick up the magnetic signature of even the most miniscule devices.

FMDS is the most reliable method of finding small electronics items (as well as other ferrous metal objects, like weapons), and should be part of the 'trust, but verify' model, in which companies assume the best of their employees and anyone else entering the building, but still take necessary precautions.

The toughest challenge in the security sector – whether it's cyber or physical – is remembering the bad guys are working assiduously to slip through the cracks, and security departments need to stay one step ahead to ward off internal and external threats. Recognising the existing threats, putting together a holistic security strategy, and using the right technology to detect illicit devices comprises an effective three-pronged approach to protecting an organisation's data.

EVERYONE AND EVERYTHING ENTERING AND LEAVING A BUILDING NEEDS TO BE SCREENED

Organisations cannot afford to be passive about security and assume employees won't steal data and spies in disguise won't sneak in. Strong countermeasures are necessary because data loss can come from both in and outside, in both private and public sectors, from places not everyone thinks of – and with technology like FMDS acting as a backup to the human element, organisations can lock down their data and keep the wolves in sheep's clothing from getting through the door ●

Douglas Miorandi is director of federal programs, counter terrorism and physical data security for Metrasens. He has 15 years of experience in electronic security consulting, design, and business development, with an emphasis on counter terrorism, surveillance, and advanced screening technology.

Small storage devices such as these can be used to steal company data and are easily concealed to avoid detection