Seth Berman argues that effective cyber resilience requires regular preparedness reviews, and warns that robust IT security is only part of the solution

THE CYBER REVIEW

©Getty Images

A survey by the UK Department for Business, Innovation & Skills has reinforced the perception that many UK businesses are woefully unprepared to combat cyber threats. The cyber governance health check tracker, which brings together the responses of FTSE 350 companies, reveals that the majority of the main boards across these organisations lack a clear understanding of the potential impact of information and data asset losses. In response, the government is stepping up its focus on highlighting the potential risks and providing a framework where businesses can identify vulnerabilities and harness best practice.

Any initiative to increase awareness and preparedness should be welcomed as the governance, financial and reputational implications of a data breach are just too important to be left as an afterthought by boards and security professionals. The threat landscape is constantly evolving and businesses must take steps to identify and understand the potential risks, irrespective of whether these are politically or financially motivated, or seemingly random.

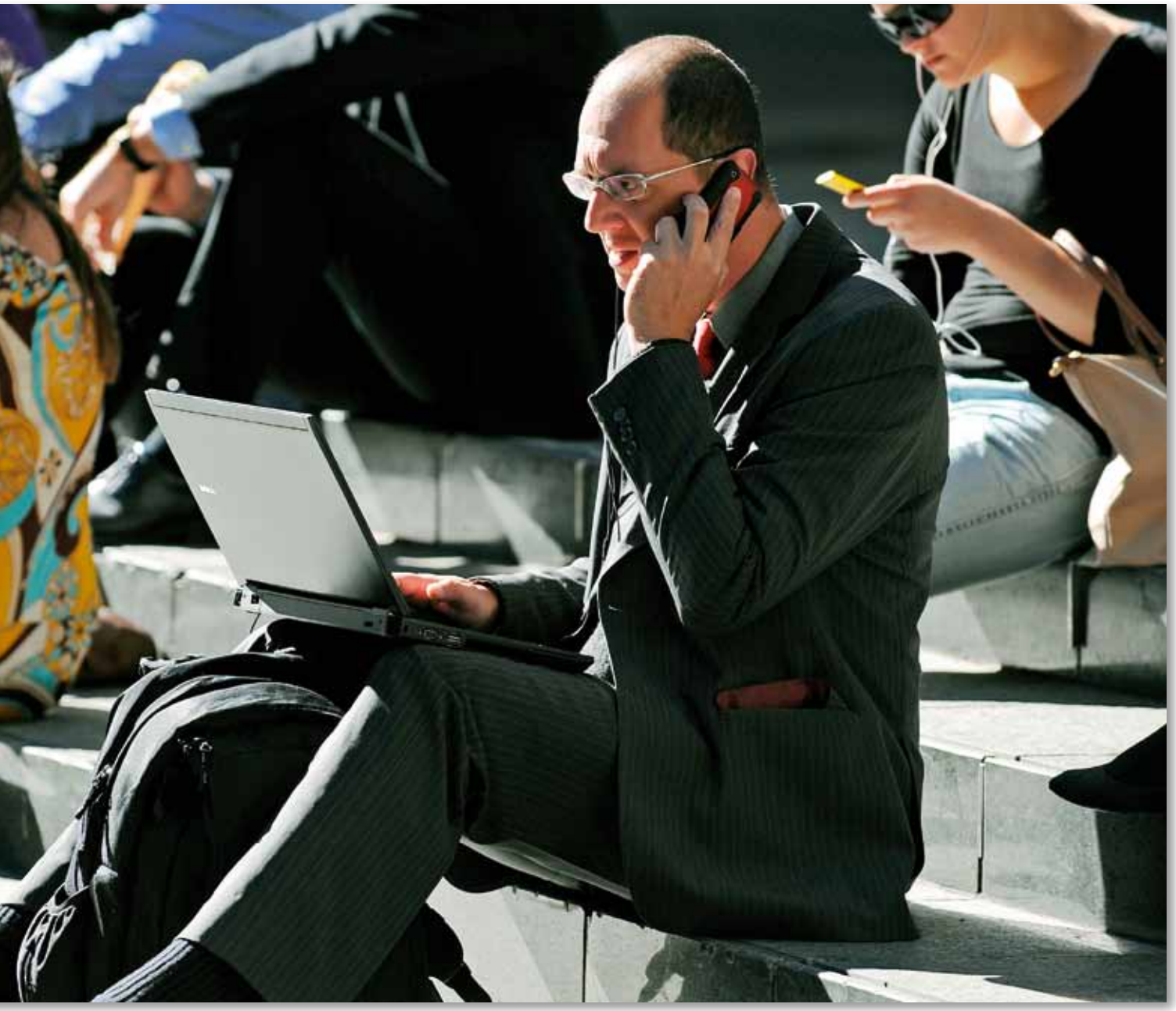
At the very heart of this strategy is the security audit, which should be carried out on a regular basis, to take into account the changing nature of cyber threats. In common with a financial audit, but not necessarily as all-encompassing, the review should be supported by external experts with the appropriate level of knowledge and insight, alongside key individuals from within the organisation. The audit will allow the effectiveness of information systems to be reviewed and appropriate remedial steps to be taken where required. It is at the heart of the process of developing a cyber security strategy and will, ultimately, allow an organisation to respond appropriately and effectively in the event of a breach.

Once ownership of the overall cyber resilience plan has been agreed, the first step should be to take stock of controls and procedures already in place. Most firms will already have firewalls, password policies, encrypted data protocols and restricted access controls to counter potential cyber threats, alongside policies governing mobile devices, cloud storage and data sharing. But when were these last reviewed, let alone tested?

Cyber risks are rarely limited to just external adversaries, with more than half of CIOs polled in one survey suggesting employees pose the greatest threat. From staff inadvertently activating viruses or malware by clicking on links in emails, to malicious insiders perhaps motivated by the prospect of financial gain, organisations will need a thorough understanding of all such threats.

The review must address everyday working practices, such as the use of personal smartphones for work-related tasks. The growing popularity of "bring your own device" (BYOD) policies has brought additional cyber security challenges. While an attractive proposition, without appropriate processes in place the BYOD strategy may create additional security headaches. As a major sports club found to its cost, the lack of clarity on the separation of personal and corporate data and usage can easily cause data protection and access issues. The club had originally issued a full set of telephones and other devices to key staff, but also allowed individuals to use personal computers and devices for work. A senior member of the club's management opted to work exclusively on his personal devices, which meant data was only backed up to the corporate network sporadically. When he left the club, however, it quickly became clear that up-to-date copies of confidential and important files were missing. With the individual objecting to his personal devices being reviewed by the ex-employer, it was left to external forensic specialists to unearth the data. This failed implementation of a BYOD policy could have caused serious data protection and reputational consequences for the club, as the private devices contained significant caches of confidential data, including medical records of players.

Despite such pitfalls, many organisations have nevertheless opted for a strategy that allows staff to use their own devices. In such cases, it is important to review the effectiveness of existing policies to ensure the employer has access to relevant information held on a specific device. There is a fine balance to be struck, as one company experienced when its BYOD policy failed to protect confidential information. Following the resignation of a member of staff who had been working on a very sensitive project, an initial attempt had been made to delete the relevant data. But, since the data resided on the individual's personal device and the employee would not grant access to it, the employer decided to use its own servers, to which the phone was still communicating, and remotely wipe the device. As a result, the former employee lost much of his personal data and subsequently made a claim against the



> More than half of CIOs polled suggested employees pose the greatest threat by inadvertently activating viruses or malware "

company for its destruction.

In assessing the wider cyber security risks, it is essential to also review current practices relating to the use of other portable devices, as the accidental loss of an unencrypted laptop or disk drive could have serious financial and reputational impact. Take for example the consultancy advising financial institutions, which allowed staff to use their own thumb drives to store business information. Months after a project with a major international bank had been completed, lawyers at the bank were mailed a drive, accompanied by a note stating that the device, which clearly contained confidential bank data, had been found on a train. Following a forensic investigation, it was established beyond doubt which of the bank's vendors had lost the thumb drive and what data had been compromised. Ultimately, personally identifiable information for many bank employees was compromised. The vendor that had

lost the drive had no idea that the data breach had occurred because it did not track the use of personal devices.

A security audit would be incomplete without assessing the effectiveness of staff in combating cyber threats. For example, are staff aware of the dangers of phishing emails, how do they react to them and what are the processes in place for incident reporting? While the vast majority may hit the Delete button, only one unwitting member of staff needs to fall for a scam before security has been breached. When the email appears to come from a senior executive, alongside a plausible explanation ("I've sent this email from my private email address as I have not been able to access the office network"), the number of individuals clicking on the offending link could be even greater.

This predicament was faced by several dozen associates at a London law firm. The email, sent after-hours from the "private" email address of the "managing partner", asked each recipient to review an attached document, the content of which would be discussed at a meeting the next morning. The document contained a virus. Once opened, the virus was deposited on the laptop of the unfortunate associate and from there onto the law firm's network. Such examples of "spear phishing" – or highly targeted fraudulent emails that may introduce a virus, activate malware to log keystrokes, copy emails, or even record phone conversations – are all too common.

Companies must, therefore, ensure they have appropriate processes in place to report all cyber security incidents to a designated team, with staff training and education a key aspect of any cyber security policy. Swift reporting allows threats to be dealt with immediately, which may also save the firm a lot of time and money in the long run. The 2013 Information Security Breaches Survey report found the average direct cost of the most severe breach suffered by large corporates was between £450,000 and £850,000, and between £35,000-to-£65,000 for SMEs. In some cases individual security breaches cost firms more than £1m in direct costs, it said. The total costs of breaches can be far higher when the cost of remediation, IP theft and reputational damage is included.

IT security is only part of the solution, however. A mistake that many organisations continue to make is to treat cyber risk as purely an IT issue. This is not only dependent on sound IT and technology controls, but also physical security, such as the use of security cameras and keyless door locks to restrict access. Any competent policy will, therefore, require a fully joined-up approach between IT and corporate security.

Cyber security will remain one of the key challenges facing organisations in the future. Risk management professionals must be at the heart of this process, to ensure such threats are understood and that the appropriate steps are taken to achieve an appropriate level of resilience. The ability to withstand an attack is rarely linked to the actual level of technology investment, however, but is a question of how an organisation is managing and regularly reviewing the resources already available, in a more effective way.

Seth Berman is executive managing director and UK head of Stroz Friedberg, an investigations, intelligence and risk management company.

Infected USB drives can deliver viruses and malware directly onto company networks