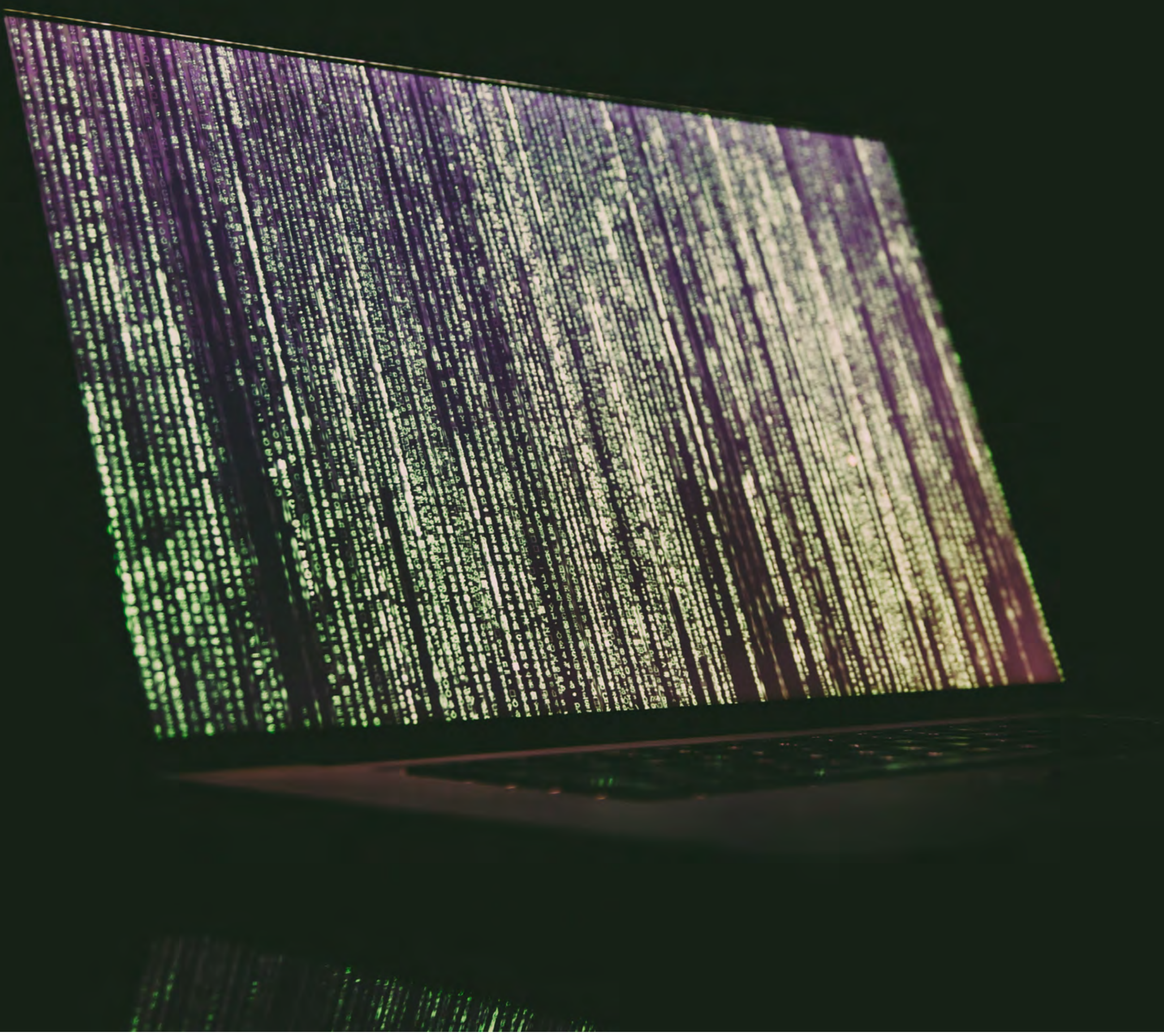
BEYOND FINANCE

CUTTING EDGE RESEARCH AND INSIGHT FROM BNP PARIBAS LEASING SOLUTIONS

WHY IT'S TIME TO UPGRADE YOUR HARDWARE



BNP PARIBAS LEASING SOLUTIONS

As featured in CBR Computer Business Review

Investing in cyber-security is a necessary precaution in the digital age.

By Tristan Watkins
CEO, BNP Paribas Leasing Solutions UK

The explosion in online fraud and cyber-crime means that IT security is getting far more attention at the boardroom table. Software vulnerabilities are addressed faster and operating systems are updated regularly. As such, the software security industry is tipped to be worth $156bn in the next five years.

All good news, except for one glaring oversight. What about hardware? Microchips run mobile phones, planes, cars, printers, electric grids and even, refrigerators. Regardless of how innocent they may seem, any of these connected devices is able to communicate with the world – and many of them are unsecured.

To keep your business and customers as safe as possible, you need to consider both your software and hardware defences.

1. OLD IT ASSETS ARE A PROBLEM

Office equipment, like any appliance or piece of machinery, is subject to wear and tear. Over time, these old assets work less efficiently and can become a major cyber-security risk. You may have the latest and most secure operating system in place, but something as seemingly innocuous as the old office printer can derail your IT security measures.

Old hard drives, memory sticks and disks all decay with time and use which can compromise your system's security. Such hardware is being built to hold more and more information and the larger the capacity, the greater the risk of 'bit' rot, data loss and downtime. Aging or 'end-of-life' (EOL) assets that store volumes of data are also prime targets for cyber-criminals as the security is often as outdated as the devices themselves.

The longer a product has been on the market; the more time cyber-criminals have had to discover its vulnerabilities. Keeping these devices protected from the latest security threats is time-consuming; malware and hackers are evolving daily and most companies don't have the resources to keep up. In other words, old assets put your company at greater risk and yet around 30-50% of IT assets installed in large businesses are past their EOL date.

Choosing to update a company's software over hardware may seem more cost and time effective, but this is a dangerous misconception that may leave your company open to cyber hacks if you fail to upgrade your hardware too.

2. HOW SECURE ARE YOUR DEVICES?

A corrupted microchip doesn't necessarily render a device inoperable. An employee's mobile phone may appear to function normally while quietly collecting and transmitting company and customer information. An infected phone can be used as a vehicle for injecting malware throughout your IT system or to coordinate with other infected devices to launch a cyber-attack. Hackers have used hardware to successfully breach security systems and read work emails, record phone calls, remotely watch and listen to business interactions using a phone's camera and microphone and, steal financial information, Intellectual property and customer sensitive data.

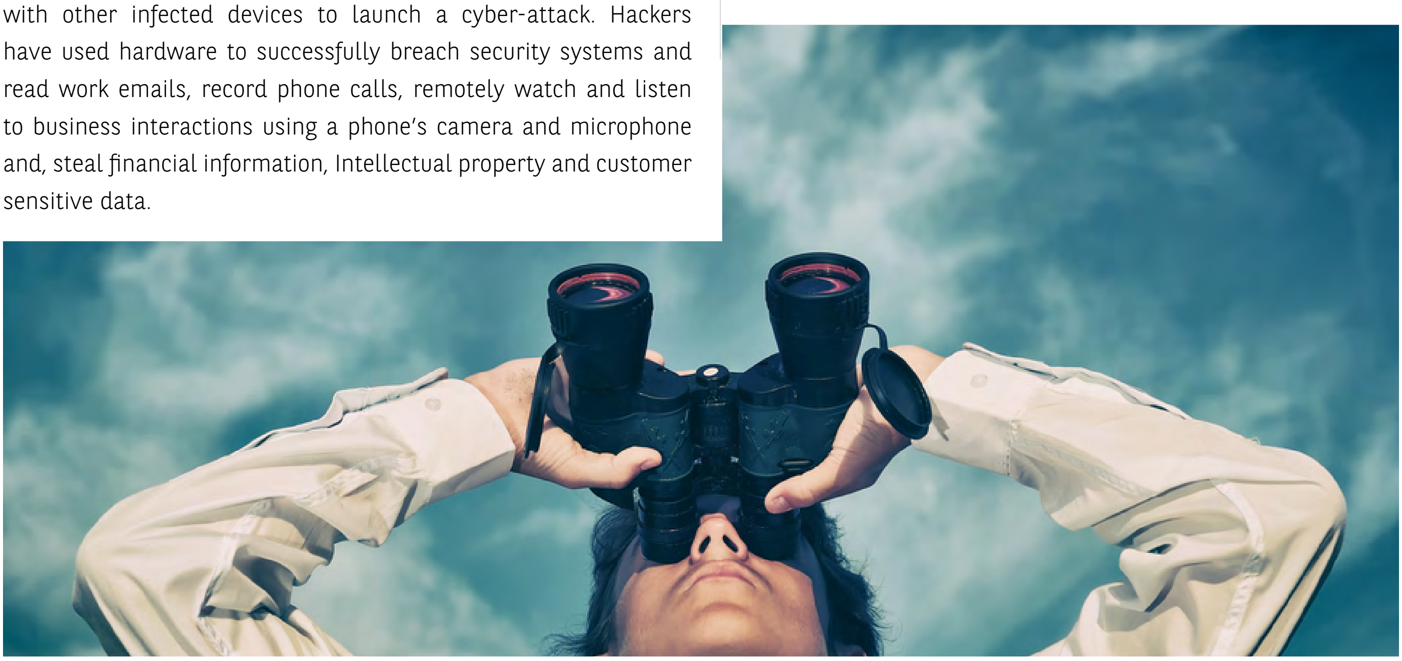
Memory sticks and disks are also high-risk. Many people use such devices interchangeably, inserting them into colleagues' or friends' devices and then back into their own with little thought given to the viruses they could pick up along the way. Of course, with more and more people working remotely or travelling for work, it's not possible to keep all office hardware on-site. Laptops, phones, memory sticks – these are all mobile devices that enable people to work anywhere at any time, but which can also leave your organisation wide open and vulnerable to cyber-crime.

3. INSIDE OUT PROTECTION

Investing in cyber-security is a necessary precaution in the digital age. Focusing solely on protecting your software is only addressing half of the problem. It's important to keep a catalogue of all office hardware and test the devices in your company regularly to ensure that they are clean and operating efficiently. A management system that accounts for all company devices, tracks their use and identifies and eliminates corrupted or unusable hardware sooner rather than later, will help protect your company from opportunistic hacks and larger cyber-security threats.

A regular review of your hardware will also make sure that all EOL assets are upgraded before becoming obsolete. Many IT resellers offer finance packages that allow businesses to spread the cost of investing in new hardware. Maintenance is also often included, as well as the ability to upgrade at the end of the lease at little extra cost, making the latest technologies accessible as and when you need them.

One of the simplest ways to help your IT department keep cyber-crime at bay is to avoid using hardware that is old, corrupted or incompatible with your software. You don't have to be a day-one adopter, but you do have stay up-to-date and make sure that your system is secure from the inside out.



TO FIND OUT HOW BNP PARIBAS LEASING SOLUTIONS CAN HELP YOU UNLOCK YOUR BUSINESS POTENTIAL PLEASE EMAIL: MARKETING.LEASINGSOLUTIONS@UK.BNPPARIBAS.COM

BNP PARIBAS
LEASING SOLUTIONS

Business is ON