SECURITY CHALLENGES IN REMOTE WORKING AND HOW TO SOLVE THEM

moon COMPUTERS

Even before the pandemic up-ended business operations worldwide in 2019, security challenges were growing for businesses of all sizes. However, the recent focus on hybrid working (the ability to work from anywhere) and the speed at which these services have been adopted have opened up businesses to even more risk.

67% OF IT LEADERS PREDICT AN INCREASE IN TARGETED PHISHING EMAILS IN WHICH CYBER CRIMINALS TAKE ADVANTAGE OF THE TRANSITION BACK TO WORKING IN THE OFFICE.[3]

In fact, the government's National Cyber Security Centre said as much themselves:

> "The pandemic has also brought about an acceleration in digitisation, with businesses and local government increasingly moving services online and essential services relying ever more on cloud IT provision. This has broadened the surface area for attacks and has often made cyber security more challenging for organisations"
> **Lindy Cameron, CEO, NCSC**

This E-book will go in-depth into these challenges and how you can overcome them, securing your business for a more prosperous future. Here's what we'll cover:

- Why are businesses more vulnerable to cyber security attacks?
- Endpoint security
- Monitoring and Maintenance
- Staff Training
- Choosing an IT Security partner

DID YOU KNOW...

Since the onset of the pandemic, employees are clicking on 3x as many malicious emails as they were before[4]

9/10 organisations say hybrid is the way forward for post-pandemic workforces[1]

Microsoft found that 99% of account hacks are blocked using multi-factor authentication (MFA), and yet 97% of M365 users don't use MFA[10]

WHY ARE BUSINESSES MORE VULNERABLE TO CYBER SECURITY ATTACKS?

In a nutshell, the more devices and networks that are used to connect to your business information, the higher the chance of one being vulnerable to an attack, or already harbouring malware unwittingly, that could then infect business devices.

THE VULNERABILITIES OF HYBRID WORKING

With your team working from home, their work laptops, personal mobiles, games consoles and anything else on their home Wi-Fi networks are all connecting to a network that is also connecting to your cloud services, which means any vulnerabilities in employees' home networks immediately become vulnerabilities in your business network.

Furthermore, home networks do not have the same level of protection that business Wi-Fi networks leverage.

Firewalls and central monitoring catch most attacks on businesses before they become problems, but with the sheer volume of new networks connecting, it can be a struggle for larger businesses to stay on top of any unusual activity found.

MICROSOFT REPORTED THAT PANDEMIC-THEMED **PHISHING AND SOCIAL ENGINEERING ATTACKS JUMPED BY 10,000 A DAY**, WHILE CYBER SECURITY EXPERTS REPORTED THAT **RANSOMWARE ATTACKS WERE UP BY 800%**[2]

AND SADLY, THE TRUTH ISN'T MUCH EASIER FOR SMALLER BUSINESSES EITHER

Even small businesses and microenterprises are at risk, especially in the supply chain of larger enterprises, as that presents an 'easier but longer' way to possibly gain access to a larger target.

One of the most successful methods of attack that hackers use is 'phishing', (sending an email that looks like it's from a reputable company, but is actually a malicious email).

These were very common at the start of the pandemic, when tensions were high and people's worries would cause them to act immediately.

In January 2022, we're now seeing these cybercriminals pivot to phishing emails themed around the tax return deadline, and you can be sure that any other similar economic challenges will be leveraged to try and access business-critical information, too.

> "Whether a phishing attack, ransomware or any other form of attack, businesses need to protect their operations from all threat types – even smaller operations."
> **Martin Brown, Technical Director, Mooncomputers**

38% OF SMES SURVEYED EXPERIENCED A CYBER BREACH OR ATTACK IN THE PREVIOUS 12 MONTHS, IN SOME CASES LOSING THOUSANDS OF POUNDS IN INCOME OR RECOVERY COSTS[NCSC]

No matter the size of a business, investing in robust cyber security tools is essential if they want to protect confidential information, keep businesses on the right side of GDPR laws, and ultimately allow businesses to grow and flourish, without having to worry about data protection!

SO, WHAT CAN BUSINESSES DO TO PROTECT THEMSELVES? FIRST, LET'S COVER ENDPOINT SECURITY...

WHY ARE BUSINESSES MORE VULNERABLE TO CYBER SECURITY ATTACKS?

Endpoint security or endpoint protection essentially means installing software or safeguards on the devices at the end of a network- the endpoint.

These could be anything from laptops to mobiles, desktops to printers, handheld devices like scanners and anything else that's connected to the business' network.

Your endpoints are all exposed constantly, and most breaches are accidental. An innocent employee may leave their phone on the bus with no passcode keeping emails secure. Or one of those emails may look like it's from the CEO, but is actually a well-crafted phishing attack tempting staff to give their login details to business-critical systems...

No matter the device or specific threat, endpoint security protects businesses from attacks resulting from both carelessness and intentional, planned breaches by ensuring all behaviour on the device is 'above board'.

EMAIL IS THE TOP DELIVERY MECHANISM FOR **96% OF PHISHING ATTACKS** AND **49% OF MALWARE ATTACKS**[8]

WHAT TYPES OF ENDPOINT SECURITY ARE AVAILABLE?

Encryption

A common way to secure data both personally and professionally by translating the information into an unreadable code, that can only be read by someone who knows the 'encryption key' to decrypt the data. If you use services like WhatsApp or Apple's iMessage, you already use encryption and any website you visit that starts 'HTTPS' – the S stand for 'secure' – also uses encryption.

In businesses, encryption could take on many forms but the principle stays the same – ensuring data is unreadable to anyone that doesn't have the encryption key. And, as one of the cheapest and most effective ways to safeguard data – we highly recommend you look to encrypt your important data, if you haven't already!

Secure Email Gateways

A secure email gateway (SEG) inspects messages that go in or out of your email platform, verifying each for any potential dangers.

When a suspicious link or file is found, the SEG prevents the email from being accessed and alerts a specified person to the issue.

This greatly reduces the chances of experiencing phishing attacks, and can help filter out other unwanted messages too, such as 'cold calling' sales emails and all the other junk mail that somehow gets through your basic email filter.

Network Access Control (NAC)

This technology, (sometimes called Managed IT Security if outsourced to a third party like Mooncomputers) focuses on managing which users and devices gain access to your network.

It also tracks the behaviours they show and the data they access, using firewalls and user permissions to safeguard sensitive sections of your network.

And if repeated concerning behaviour is identified, an IT team knows an attack is (or will soon be) underway, and further steps, such as sandboxing (when affected systems are locked out of all other connected systems) to limit access to data and isolating it for further investigation.

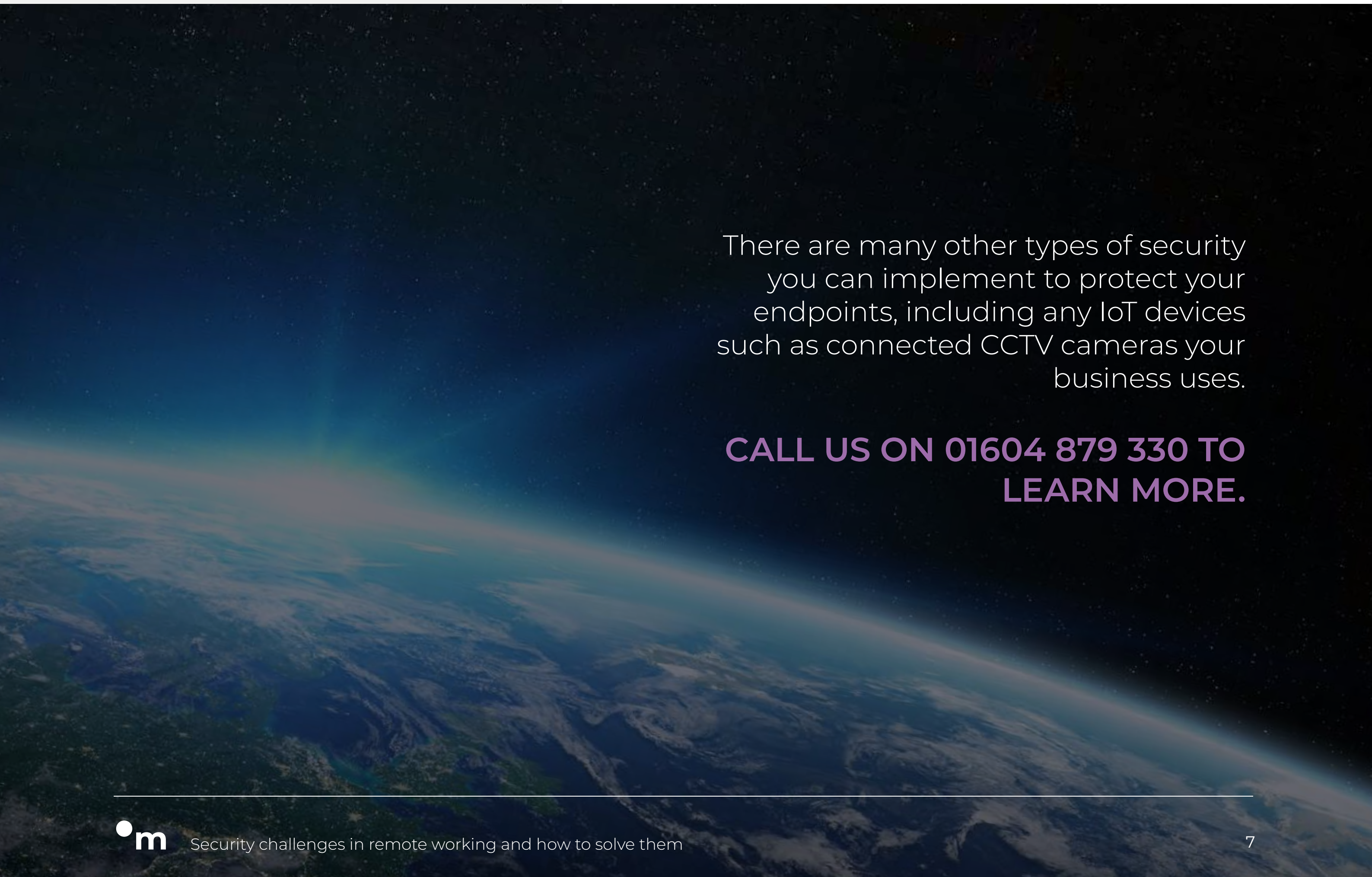
Data Loss Prevention

A data loss prevention (DLP) strategy focuses on ensuring that your most secure data resources are protected against exfiltration.

One of the best ways to safeguard these assets is to keep employees informed about phishing tactics, as well as installing antimalware to prevent data loss from malicious programs hackers install on your endpoints.

A strong DLP strategy doesn't just help cybersecurity. It helps your overall data safety by ensuring all data is backed up to at least one other location, ensuring that no matter the cause – flood, fire, theft or cyberattack – that your data is safe. Which makes it a highly recommended focus for businesses of all sizes.

70% OF BREACHES ORIGINATE AT THE ENDPOINT, BUT **42% OF ALL ENDPOINTS ARE UNPROTECTED** AT ANY GIVEN TIME[6]



There are many other types of security you can implement to protect your endpoints, including any IoT devices such as connected CCTV cameras your business uses.

CALL US ON 01604 879 330 TO LEARN MORE.

MONITORING AND MAINTENANCE

As we mentioned earlier, monitoring your network for any unusual activity is important, otherwise you don't know what data is going where, or who's looking at it. However, many businesses do not have the resources or expertise to effectively monitor their own network activity, and threats will continue to challenge businesses far into the future, meaning businesses need to stay on top of those advances. Thankfully, there are software systems that can monitor network activity automatically, however, they still need a knowledgeable administrator to verify threats identified and mitigate them.

Plus, monitoring is only half the story as maintaining your network and connected devices is another vital factor in implementing a robust security policy across any business. So, for many SMEs and microenterprises, monitoring and maintaining a business network is simply impossible, which should not be the case in the modern digital economy. And even with a robust IT team like the NHS', there are still issues with in-house cybersecurity management. Here's our real-world example, that proves just that:

REAL-WORD EXAMPLE:

Back in 2017, the WannaCry attack brought 80 out of 236 Primary Care Trusts to their knees, as well as 603 primary care and 595 GP practices, all infected with malware that locked users out of their systems until a ransom was paid...

Sadly, the whole issue could have been prevented if the NHS had properly maintained their devices. The version of Windows (XP) that the NHS had been using was no longer supported in lieu of more recent versions (Windows 7 and 8).

This meant that security gaps that had been fixed in more recent Operating Systems were still open to malicious activity.

This proves just how important those annoying little updates on phones and computers are.

While missing one or two updates typically don't cause major vulnerabilities (and of course we recommend you update devices as soon as prompted), it's easy for businesses to forgo these updates due to time, resource challenges and focus on more business-critical goals.

WHILE THE NHS NEVER PAID THE RANSOM AND WAS GIVEN BACK ACCESS TO ALL SYSTEMS, ESTIMATES PUT THE **TOTAL COST OF THE ATTACK AT £92M**!

That's why many businesses outsource their IT security and network management to an experienced third party instead.

VISIT MOON.CO.IT/IT-SECURITY TO LEARN ABOUT OUR MANAGED SECURITY SERVICES.

STAFF TRAINING

We've mentioned a couple of cost-effective ways to protect your data such as a Data Loss Prevention strategy, encryption and robust maintenance policies, but another is far simpler –training to your staff!

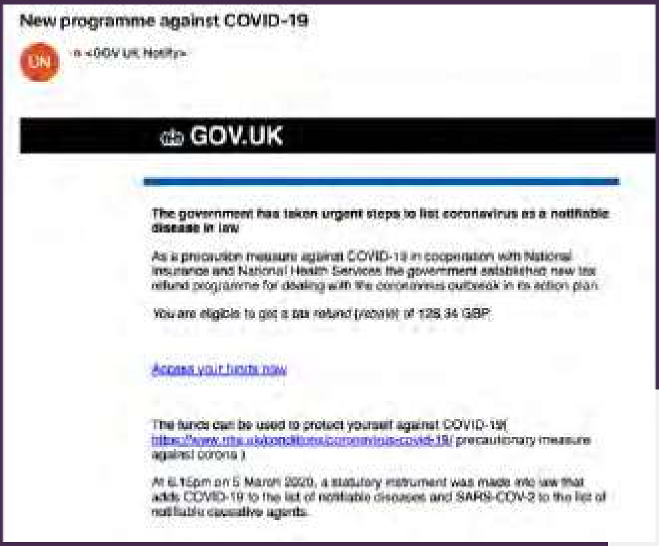
AS OF EARLY 2021, **86% OF UK BUSINESSES HAVEN'T HAD TRAINING** OR AWARENESS SESSIONS ON CYBER SECURITY IN THE LAST 12 MONTHS[5]

We find this stat incredibly eye-opening. While we fully understand that businesses had to quickly transition to a hybrid working strategy and keep staff productive, training staff is essential to mitigate the risks that hybrid working presents.

Especially considering that phishing attacks are the most common attack strategy to gain access to businesses, basic training on how staff can identify these emails goes a long way to protecting data and limiting the financial costs of an attack.

SECURITY **RISKS ARE REDUCED BY 70%** WHEN BUSINESSES INVEST IN SECURITY AWARENESS TRAINING[9]

TAKE THIS REAL-WORLD EXAMPLE:



New programme against COVID-19

UN n <GOV UK Notify>

GOV.UK

The government has taken urgent steps to list coronavirus as a notifiable disease in law

As a precaution measure against COVID-19 in cooperation with National Insurance and National Health Services the government established new tax refund programme for dealing with the coronavirus outbreak in its action plan.

You are eligible to get a tax refund (rebate) of 128.34 GBP.

Access your funds now

The funds can be used to protect yourself against COVID-19(https://www.nhs.uk/conditions/coronavirus-covid-19/ precautionary measure against corona)

At 6.15pm on 5 March 2020, a statutory instrument was made into law that adds COVID-19 to the list of notifiable diseases and SARS-COV-2 to the list of notifiable causative agents.

As you can see, the 'email address name' doesn't look particularly irregular, but should start prompting questions...

There are multiple grammatical errors and no name of the receiver included. These are both major red flags, meaning anyone who has had decent training would identify this as a phishing attack

86% OF UK BUSINESSES HAVE NOT HAD END USER TRAINING SESSIONS IN THE LAST 12 MONTHS, EVEN THOUGH END USERS ARE THE #1 CAUSE OF DATA BREACHES[5]

CHOOSE A SECURITY PARTNER THAT'S OUT OF THIS WORLD!

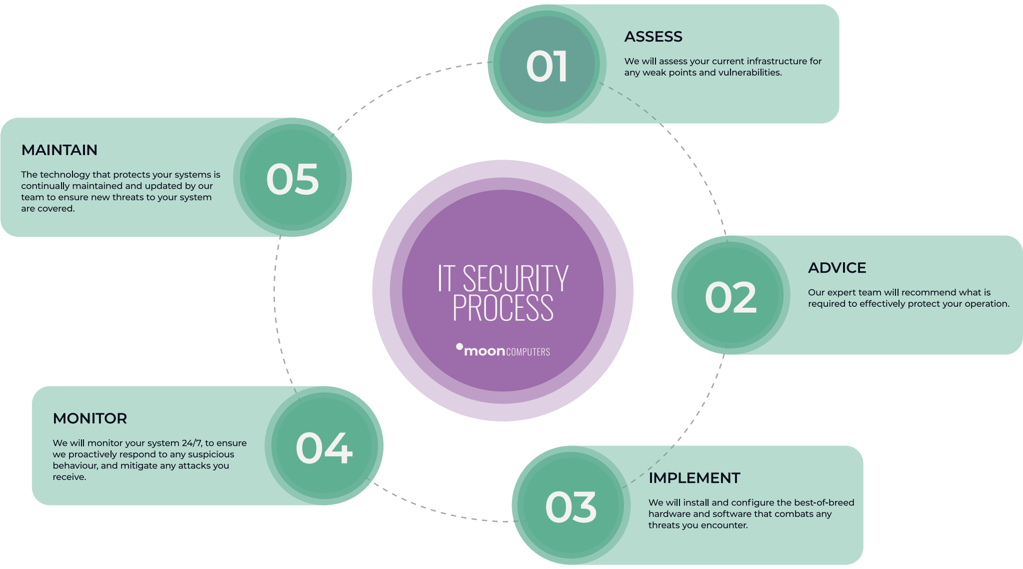
As we've discussed, many businesses may not have the time, staff or available resources to manage their network security themselves. That's where Mooncomputers can help.

54% OF IT DECISION MAKERS ARE WORRIED REMOTE WORKERS WILL BRING INFECTED DEVICES AND MALWARE INTO THE OFFICE[3]

WHY CHOOSE MOONCOMPUTERS?

Our specialised technical team have the tools, knowledge and skillset to effectively mitigate the threats that your business is vulnerable to, ensuring robust cybersecurity policies are in place and properly maintained. With vast experience, accreditation and continual development and learning, we keep abreast of any recent developments in the security industry to maintain our exceptional levels of protection. And everything we do is guided by our 5-step process:

OUR IT SECURITY PROCESS



IT SECURITY PROCESS

•moonCOMPUTERS

01 ASSESS

We will assess your current infrastructure for any weak points and vulnerabilities.

02 ADVICE

Our expert team will recommend what is required to effectively protect your operation.

03 IMPLEMENT

We will install and configure the best-of-breed hardware and software that combats any threats you encounter.

04 MONITOR

We will monitor your system 24/7, to ensure we proactively respond to any suspicious behaviour, and mitigate any attacks you receive.

05 MAINTAIN

The technology that protects your systems is continually maintained and updated by our team to ensure new threats to your system are covered.

If you want a stellar service and robust IT security for your business, the best decision you can make is calling our expert team and joining the growing constellation of UK businesses that trust Mooncomputers with their most valuable asset – their data.

SOURCES

1. What Executives are Saying About the Future of Hybrid Work, McKinsey, 2021
2. Top Cyber Security Executive Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic, PR Newswire, 2020
3. Back to Work - Security Behaviours Report, Tessian, 2021
4. The State of Email Security 2021, Mimecast, 2021
5. Cyber Security Breaches Survey 2021
6. 2019 Endpoint Security Trends Report
7. Overconfident, underprepared...and asking for trouble, Bullguard, 2020
8. A Visual Landscape of Cybersecurity. Optiv Security Inc., 2019
9. Infographic: 10 statistics that show why training is the key to good data protection and cybersecurity, Pensar, 2018,
10. 97% of Office 365 Users Don't Use MFA, UK Cyber Security Council, 2020

We believe in cultivating relationships that can stand the test of time. We know it’s important to maintain great process and communications with our customers.

CALL US ON 01604 879 330 TO LEARN MORE ABOUT IT SECURITY

moonCOMPUTERS

Mooncomputers Ltd,
7 Prospect Court,
Courteenhall Road,
Blisworth,
Northamptonshire,
NN7 3DG

01604 879330
info@moon.co.it