Cyber
Training Guide

Know the threats to your business

brother at your side | in[ctrl]

In partnership with KnowBe4
Human error. Conquered.

The global average cost of a data breach in 2023 was $4.45million / £3.51million / €4.05million[1] – 15% increase over 3 years.

When remote work is a factor in causing a data breach, the average cost per breach is $173,074 / £136,500 / €157,506[2] higher.

54% of companies say their IT departments are not sophisticated enough to handle advanced cyber attacks.[3]

If hackers tried to breach your cyber defences today, would they be successful? If you can't immediately be confident in the strength of your organisation's cybersecurity, you've got a big problem. And you're not alone. Maintaining secure IT systems remains one of the greatest challenges for IT decision makers (ITDMs). And with cyberthreats increasingly sophisticated and organisations more reliant on digital systems than ever before, the risk of a successful attack has never been greater.

Following Brother research, we've identified that unfortunately, many IT departments feel woefully unprepared. Lack of budget and the appropriate resources/tools are some of the most cited reasons why many ITDM's are concerned about arising cybersecurity attacks and their ability to defend successfully against them.

54% of ITDMs say that budget spend on maintaining secure IT systems is growing.

Nevertheless, 44% still feel that maintaining secure IT systems remains their greatest challenge, indicating that budgets probably aren't being spent wisely.

We've used Brother data and partnered with KnowBe4 to highlight some of the risks facing businesses today, and how implementing a culture of training and security knowledge can keep businesses safe and prepared for possible threats.

Humans are the last line in defence when it comes to the cybersecurity of any organisation, and while IT departments are ultimately held responsible for any issues with cybersecurity, the reality is that every single person who works within an organisation has a degree of responsibility for preventing breaches. Making sure that employees understand this and providing the education and training to be aware of cybersecurity threats and what to do to avoid them, should form an integral part of any organisation's cybersecurity strategy.

Human error is a major contributing cause in 95% of cyber breaches.[4]

Basil Fuchs
Chief Information Officer
Brother International Europe

"Risks to cybersecurity are only increasing – something that is a direct result of cyber criminals becoming more sophisticated with social engineering to instigate attacks. People are getting pre-texted about scam emails before they even arrive in their inbox to make them seem more legit. And cyber criminals are playing on employee's need to work at speed, and not having time to carefully analyse messages for tell-tale signs of a scam".

[1]IBM [2]IBM [3]Sophos [4]IIBM Cyber Security Intelligence Index Report

The biggest threats facing businesses

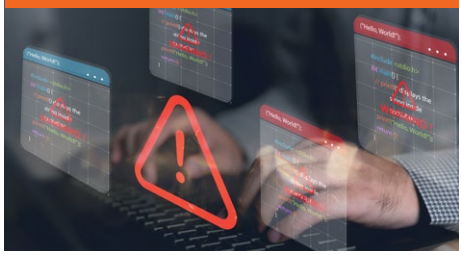
Brother has undertaken thorough research with ITDMs across Europe and asked them about the cybersecurity threats that they are facing and feel underequipped to deal with. Perhaps unsurprisingly, they are all areas where human error can play a part in a successful attack.

In this guide, we take a look at the three most commonly identified cybersecurity threats that ITDMs feel least-equipped to deal with, and the tools and techniques that your organisation can adopt to bolster your defences and minimise the risk of a security breach.

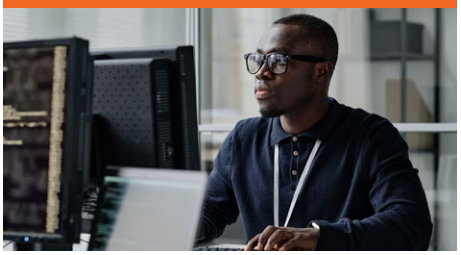
These threats include:

Phishing Attacks

Malware



Network Security



However, one of the greatest challenges facing ITDMs is the need for training to strengthen these areas, with many not having the time or budget required. But with humans as the last of defence for each of them, it's imperative that teams are taught how to identify and respond to risks quickly and accurately. Without the necessary in-house resources, many businesses like Brother are choosing to appoint partners to fill the gap.

Russell Johnson
Business Partner and Global Cyber Security Lead
Brother International Europe

"It is easy for businesses to think they can tackle security training by themselves, and letting an external party in on your cybersecurity practices can seem to go against the very idea of effective cyber defences, and for this reason, many organisations prefer to keep training and development on this integral part of their business operations in house.

However, unless your inhouse teams are aware of up-to-the-minute techniques used by hackers, you can't successfully train your employees on the best way to maintain your cyber defences, and it can leave your business systems vulnerable to attack."

People play the biggest role in keeping an organisation secure

We asked about IT issues becoming more or less challenging in our research too, and 50% of ITDMs said maintaining secure IT systems is becoming more challenging. Hackers are constantly developing new tools and techniques to breach cybersecurity defences, making it extremely difficult for organisations to identify and effectively protect against the latest approaches. Meanwhile, the growth of the Internet of Things (IoT) continues to create many new targets for hackers to exploit.

With so many access points into a business, and large numbers of people working online across multiple devices and locations, it's the people within an organisation that are often the weakest link in any cybersecurity strategy. Whether it is from a lack of training, forgetting or simply failing to follow cybersecurity best practices or being tricked by cybercriminals and whilst employees are your greatest asset, they can also be your greatest liability.

Only 29% of ITDMs would put user security training at the top of their priorities.

Just 1 in 9 UK businesses provided cybersecurity training to non-cyber staff in 2022.

Javvad Malik
Lead Security Awareness Advocate
KnowBe4

"Technology and training intertwine in security awareness by leveraging digital tools to deliver comprehensive education. Technology facilitates interactive modules, simulated phishing exercises, and access to online resources, ensuring employees grasp cybersecurity principles effectively. Training complements this by instilling critical thinking and best practices, empowering staff to recognise and respond to threats. Together they create a dynamic learning environment where employees not only understand cybersecurity risks but also develop the skills to mitigate them. Regular updates and feedback mechanisms ensure alignment with evolving threats, fostering a culture of vigilance and resilience within the organisation."

Hackers have no scruples about attacking any size of organisation. However, it tends to be small and medium-sized businesses who aren't comfortable making significant investments in defensive cybersecurity that could be at greatest risk. And with remote work more common than ever, it's particularly challenging for businesses to make sure that their employees are following best practice when it comes to cybersecurity.

Creating a culture of cybersecurity within your organisation

Regular cybersecurity training should form an integral part of any employee's continuing professional development (CPD). However, this isn't as common as it should be.

Effective cybersecurity training is about more than just putting employees through awareness programmes intermittently. Organisations that are truly prepared for attacks, and have the best defences against them, have cybersecurity embedded within their culture, and employees who subconsciously strengthen their defences day in day out.

Russell Johnson
Business Partner and Global Cyber Security Lead
Brother International Europe

"Brother is committed to creating a culture of cybersecurity across the breadth of its organisation. That's because we understand that cybersecurity isn't a tick-box exercise. It's a collective and constant responsibility. Our cybersecurity is only as strong as our people, and so as an organisation, the best way to protect ourselves is to invest in them and give them the knowledge and skill they need to identify and respond to cyber threats, whenever and wherever they occur."

60% of SMB ITDMs claim that the IT department is responsible for business-wide cybersecurity training.

Russell Johnson
Business Partner and Global Cyber Security Lead
Brother International Europe

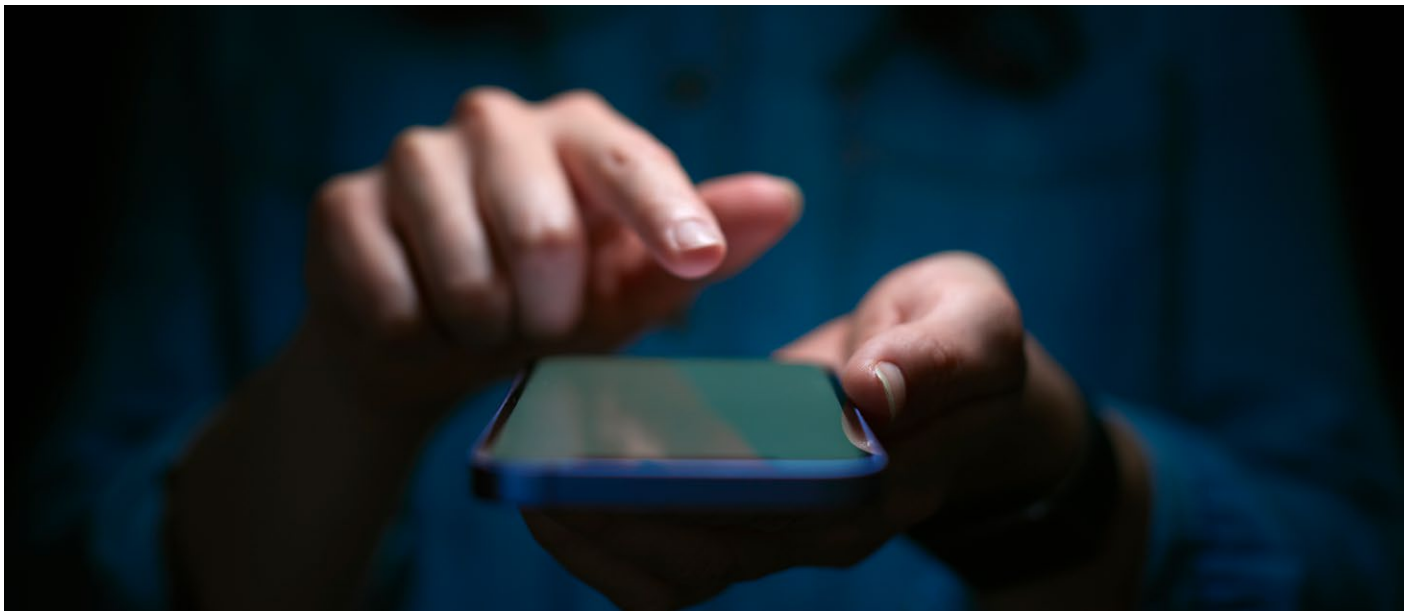
"Over the last few years, we've drastically ramped up our cybersecurity awareness within Brother through security proficiency awareness testing and automatic remedial training that's highly targeted and based on identified user weaknesses. We supplement this with fortnightly or less articles based on current cybersecurity news and trends, and quarterly techbars that use interactivity and guest speakers to really engage our teams with the latest developments to be aware of."

Top tips for engaging your employees in cybersecurity

Research suggests that IT departments are responsible for creating a cyber security culture within any organisation, which can be difficult for those with limited knowledge and resources. That being said, steps should be taken in every organisation to protect them.

This means:

- Creating content and training materials that resonate with colleagues across the business, at differing skill levels
- Making sure the content they use to deliver the training is clear, relevant and backed by real world examples that demonstrate it in action
- Delivered it in a format that everyone in their audience can connect with, and that makes the information memorable
- Using different techniques to make cyber education part of the company culture – such as newsletters, videos, posters and even events
- For global organisations, ensure that content isn't only translated appropriately, but also region-specific to users to have the greatest impact
- Fostering good relations between IT and colleagues across the business, providing positive feedback and kudos to those who report suspicious behaviour or emails, so they know their contributions are appreciated
- Encouraging leaders to share their experiences and lead by example.



Phishing attacks

Phishing is when a cybercriminal poses as a legitimate person or business, usually by email, social media or phone, to try and obtain sensitive information such as passwords or credit card numbers. It's also used as a delivery tool to spread malware. Phishing remains one of the most popular social-engineering forms of cyberattack.

74% of all data breaches include the human element.[5]

Since organisations rely heavily on digital communication channels, it is a perfect avenue of exploitation for cyber criminals. However, avoiding a phishing attack relies almost completely on your employees being able to recognise a phishing attack and avoid it.

Unfortunately, phishing scams usually involve impersonating well-known brands such as Microsoft, Amazon, DocuSign and Google to trick users. In fact, more than 30 million messages using Microsoft branding or mentioning Microsoft products were used in phishing attacks in 2022.[6]

28% of SMB ITDMs say that phishing attacks are the cybersecurity breach that they feel least equipped to deal with.

96% of UK companies are the biggest target for phishing attacks in Europe, followed by 94% of companies in Spain, 85% in France and 79% in Italy.[7]

[5]Verizon's 2023 Data Breach Investigation Report [6]Forbes, 2023 [7]IT Governance

How can ITDMs secure themselves against phishing attacks?

Since phishing attacks exploit human weaknesses, the only real way to try and secure your organisation against them is to make sure that all employees are properly trained to spot them and know what to do if they suspect one. And since phishing attack methods are constantly evolving, training and education on the latest phishing techniques shouldn't be viewed as a one-off event, but a regular update given to all employees, regardless of their role within your organisation.

As an added layer of protection, ITDMs can also implement phishing protection software solutions. These work by analysing various elements of messages, and flag or block suspicious content, stopping it from reaching your inbox or web browser.

Phishing red flags

A successful phishing attack is based on the need to trick employees into clicking on and/or sharing something that they shouldn't. The only way to prevent them from doing this is through regular training and reminders about "red flags" that could indicate a message is a phishing attempt.

Red flags they should look out for include:

- A message that comes from a domain that isn't the same as the company it's supposed to be from
- Mismatched URLs in a website address
- Spelling and grammatical errors
- Unusual fonts, especially if the font seems to change midway through a word
- The attempt to create a sense of urgency: "this link expires in 48 hours" or "hurry to validate your identity"
- Unusual greetings, such as "Hi dear".

How good are your teams at spotting a phishing email or message? They used to be fairly easy to spot thanks to obvious spelling and grammatical errors, but thanks to generative AI helping scammers overcome these issues, detecting phishing messages is becoming harder than ever. One way to find out how prepared your teams are is to establish your Phish-prone™ percentage.

Regular phishing tests should therefore form an integral part of any organisation's cybersecurity plan.

Russell Johnson
Business Partner and Global
Cyber Security Lead
Brother International Europe

We've implemented a variety of steps to minimise the risk of experiencing a phishing attack. Some of the phishing simulation that we've deployed as part of our cyber strategy include:

- HR-orientated emails, using things like sickness, annual leave and signing new policies
- Manager-orientated emails, such as asking employees to quickly open/read/sign documents
- System-oriented emails, like links to sign a Google doc, or access to a SharePoint."

Phish-prone™ percentage: What is it and why is it important?

Your Phish-prone percentage refers to the percentage of employees that are prone to clicking on a phishing link or interacting with a phishing message in an unsafe way. This could be entering data on a fake landing page, opening an attachment or replying to the message.

The phish-prone percentage is calculated by dividing the number of employees who fell for a phishing test by the number of employees who were tested. The result is then multiplied by 100 to get the percentage. For example, if an organisation has 100 employees and 20 of them clicked on a phishing email during a test, the phish-prone percentage would be 20%.

"Don't panic if your Phish-prone score is higher than you expect – it's fairly common if you've not been phish-tested before. At Brother, we've been able to reduce ours considerably over a fairly short space of time using a series of training tools and simulated phishing tests. In fact, we're now hitting our industry benchmark of 6%, which proves the impact that constant testing and regular training can have."

Phishing tests and training in action

Phishing tests are one of the most effective ways of discovering just how prepared your teams are to deal with a phishing attack should your organisation be targeted, and to reduce your organisation's Phish-prone score.[8] The premise is simple. Businesses looking to test staff set up simulated phishing tests (in house or via a specialist partner) that try to trick your people into giving away sensitive information, but without any actual risk. There are multiple ways in which they try to obtain this information, and at the end of the tests, your Phish-prone percentage is calculated and compared to others in your industry (a benchmark figure).

Javvad Malik
Lead Security Awareness Advocate
KnowBe4

"KnowBe4's 2023 Phishing by Industry Benchmarking Report reveals that 33.2% of untrained users will fail a phishing test. However, by implementing security training and committing to developing a culture of cybersecurity, businesses have shown that it's possible to reduce this to below the industry benchmark of 5.9%."

Russell Johnson
Business Partner and Global Cyber Security Lead
Brother International Europe

"At Brother, we've consistently reduced our phish prone percentage in recent years. How? We began with a baseline phishing test in March 2022 which showed that our Phish-prone percentage (PPP), was 11.5%. Following this, we implemented robust training and security proficiency awareness testing to identify key areas of weakness. We were then able to arrange remedial training based on this to close any gaps. We've sent more than 30k phishing emails, with 17k sent in the last 12 months. At present, our PPP is just 5.2%, with a target of <2%."

The industry benchmark for phishing is built in three phases:

Phase one: A simulated phishing email is sent to all users where they have not received any prior training. The percentage of people who fall for the phishing email will give the baseline percentage. On average, globally 33.2% of employees will fall victim to the phishing email.

Phase two: Users have completed training and received phishing tests, 90 days after the initial phish.

Phase three: The test is repeated after 12 months.

What the data shows, based on 32.1 million phishing emails to 12.5 million users is that phishing security test results after 90 days of training globally drop from 33.2% to 18.5%. This further drops to 5.4% after 12 months.

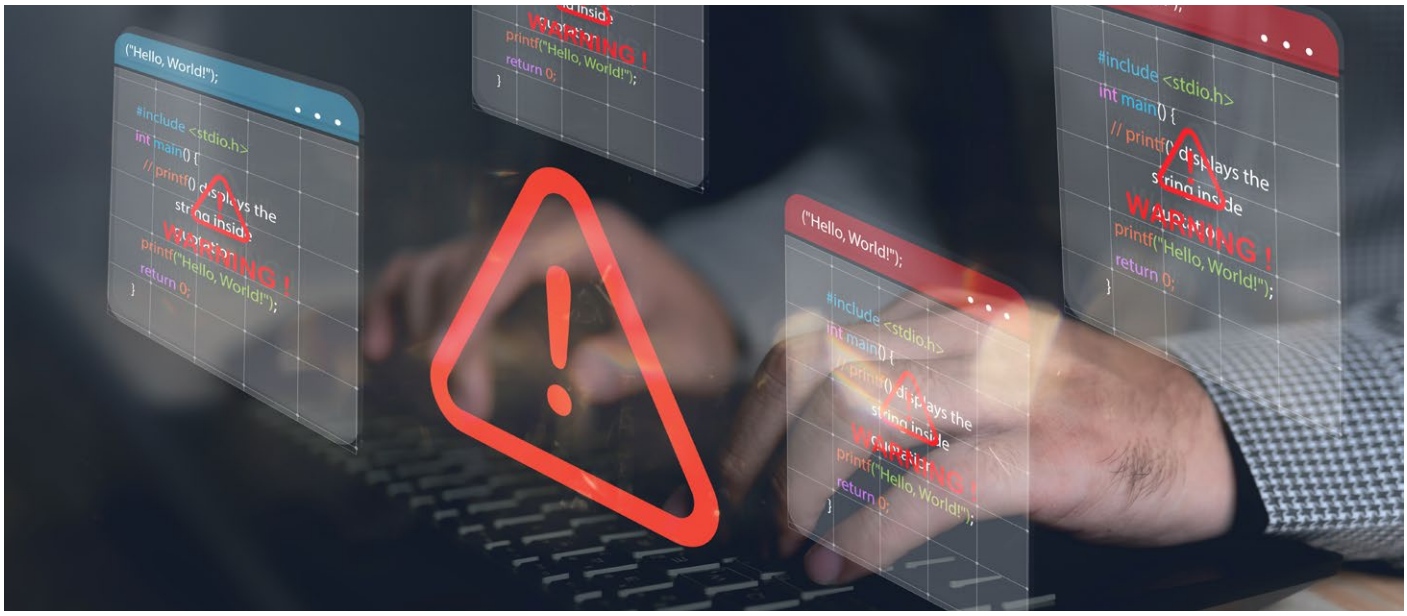
These percentages will vary depending on the industry, location, and size of organisation.

91% of successful data breaches start with a spear-phishing attack.[9]

What is spear-phishing?

Spear-phishing is a type of phishing attack that targets specific individuals or organisations typically through malicious emails. The goal of spear phishing is to steal sensitive information such as login credentials or infect the targets' device with malware.

[8]KnowBe4 [9]KnowBe4



Malware

One of the biggest challenges that ITDMs feel that they face is the threat of a very specific type of software, called malware, penetrating their IT infrastructure.

34% of SMB ITDMs say that malware/ransomware are the cybersecurity breach that they feel least equipped to deal with.[10]

What is Malware?

Malware is software that is designed specifically with the aim of disrupting, damaging or gaining unauthorised access to a computer system. As we know, phishing attacks are often used as a way of getting malware onto your systems – by getting you to click on a link in a phishing message or download attachments that you don't realise are malicious.

Other ways in which malware can get onto your device include:

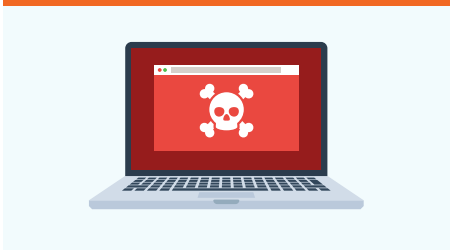
- Automatic downloads from compromised websites
- Infected software being installed onto your device
- Removable media: USB drives and external hard drives
- Outdated software that has security vulnerabilities.

There were more than 100,884,532 known records breached in Europe in December 2023.[11]

[10]2023 Brother X Savanta ITDM priority survey [11]IT Governance

The most dangerous types of malware: an overview

Trojans



A Trojan is a virus that can damage your files, modify your data, monitor your activity, steal sensitive information from your device, redirect internet traffic, or even set up backdoor access points to your systems – all without your knowledge.

Ransomware

Ransomware is a type of malicious software that is designed to block access to your device and the data stored on it until you pay a ransom to the attacker. They usually do this by encrypting your files so you can no longer see or use them.

Worms

Worms are a type of Trojan virus, but their primary function is to self-replicate and infect other devices, while also remaining active on any systems that they've previously infected.

How can ITDMs secure themselves against ransomware attacks?

In January 2023, Royal Mail was attacked by one of the most dangerous ransomwares in the world – LockBit – where the ransom demand was $80 million.[12]

As we know, many ransomware attacks are delivered via successful phishing attacks, where users click on illegitimate links that download unsafe software onto their device. This means that one of the most effective ways of securing your organisation against this type of threat is to ensure your teams know how to spot and avoid phishing attacks. And partnering with a trusted partner can tell you exactly how effective your teams are at identifying them.

Other steps you can take to avoid ransomware attacks include:

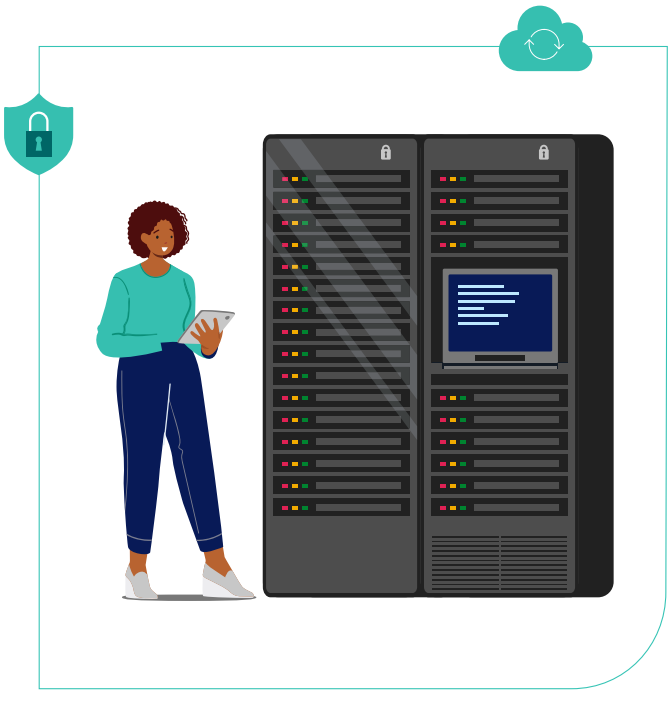
- Keeping software up to date
- Deploy two-factor authentication, particularly for remote workers
- Ask users to change their passwords regularly
- Use security hardware and software including firewalls, email-scanning applications and antivirus software
- Perform regular back-ups and store everything in a separate network environment.

Javvad Malik
Lead Security Awareness Advocate
KnowBe4

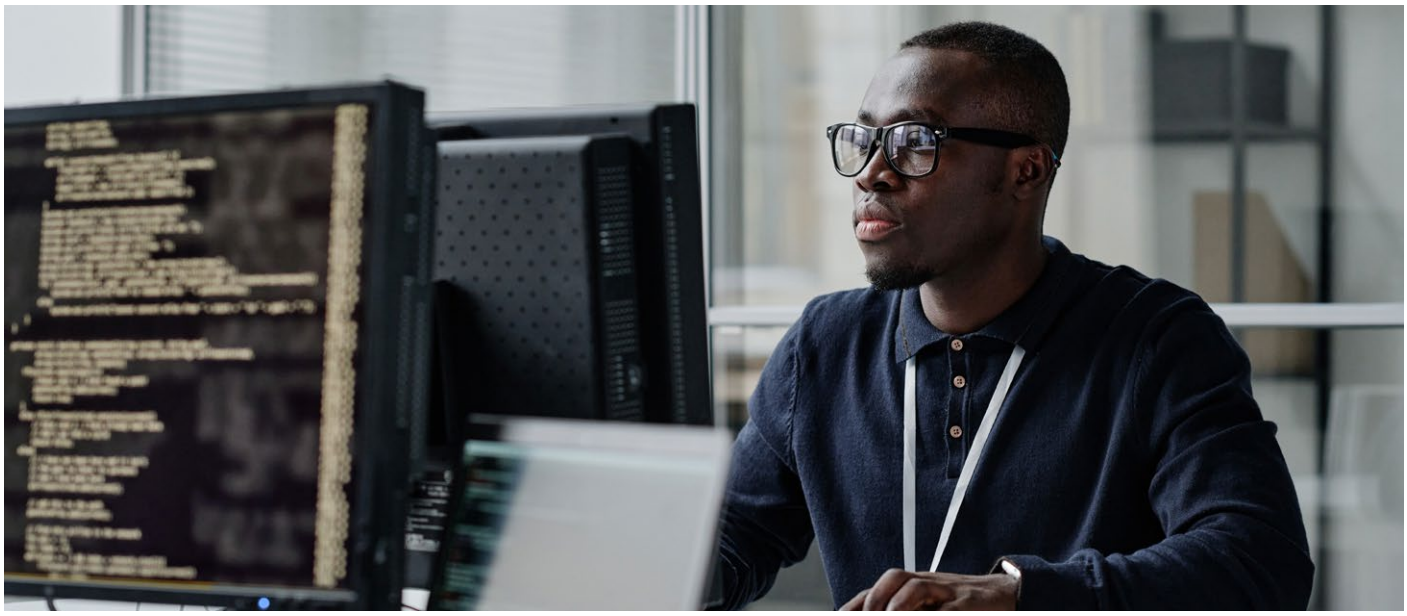
"To beat Ransomware, organisations can use tools such as, RanSim, to give a 360° view of their preparedness for an attack. RanSim simulates 24 different ransomware infection scenarios and one cryptomining infection scenario to determine if a workstation is vulnerable."

Another option is to implement SOAR – Security Orchestration Automation and Response. SOAR that is designed specifically for phishing threat responses and management can reduce your Mean Time To Respond (MTTR) and mitigate phishing threats before they make it to your teams' inboxes.[13] This proactive attitude to phishing is further supported by capabilities such as:

- Automated email responses that enable IT departments to communicate with employees quickly, reducing operational downtime
- Pattern identification that enables your incident response teams to identify widespread attacks quickly
- Taking real-world attacks and turning them into training model simulations to enhance the skills and experience of your employees.



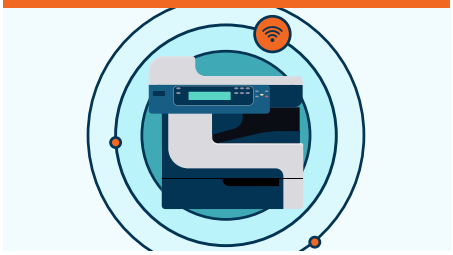
[12]bbc.co.uk [13]KnowBe4



Network security

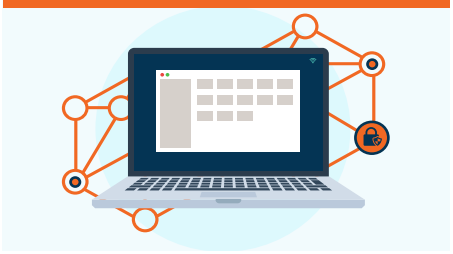
Something that is often overlooked by businesses is network security. We know this is an issue that can have huge implications. However, from our research, it's clear this is often an overlooked priority. Network security refers to the processes and software that you use to protect your computers, printers, network and data. It's generally broken down into three areas:

Physical



Security controls used to stop unauthorised access to physical networks like printers, routers and hard-drives (endpoints).

Technical



Security that protects data coming in, going out and stored on the network.

Administrative

Security controls for user behaviour, such as who has access and what authentication steps are used.

The least secure part of any network is the endpoint. Again, this is where users come into play. Hybrid working has created new challenges for organisations and network security. Remote workers are likely to access company servers over public networks, which offers far less protection. There's a bigger attack surface with increased entry points for cybercriminals. It;s also harder for IT teams to identify and respond to attacks.

Basil Fuchs
Chief Information Officer
Brother International Europe

"In today's digital and flexible work landscape, securing networks is crucial to protect sensitive data. The Zero-Trust model, which assumes no inherent trust, ensures that all users and devices are verified before granting access. By limiting access to only what's necessary, this approach reduces the risk of unauthorized lateral movement".

Zero trust network access is a highly effective security model that ensures that users only have the access and permissions needed to fulfil their role. It's a very different approach to standard VPNs that grant all users access to the full network. The benefit of a zero trust approach is that if any user is compromised, hackers will only be able to access the data that they are privy to, and not the network as a whole.

We've also put together some quick wins on ways to improve your network security:

1. Use SSL certificates
2. Ask remote workers to encrypt their home wireless network with WPA2 encryption
3. Change your router's name and password to mask your identity
4. Disable WPS on routers
5. Send reminders to all users to back up their devices including printers, scanners etc regularly, and to install updates as soon as they are available.

How to approach network security

Network security encompasses many different elements, each as crucial as the other. This is particularly true in the era of hybrid and remote working, where it's just not possible for ITDMs to visit and check home set-ups or even see their people in person with any regularity. With this in mind, here are our top tips to make sure you've got all the bases covered.

Use SSL certificates

An SSL (Secure Sockets Layer) certificate and using HTTP if you do any sort of selling via your network, is essential. An SSL certificate ensures no data that's being shared between your servers and clients can be stolen by a third party, while the certificate confirms the identity of the server and sets up an encrypted communication channel to enable purchases.

Keep your router firmware up to date

This is particularly important for remote workers, since router firmware comes pre-installed on their devices. Router firmware should be updated at least once every year to offer the best defence against cyber threats.

Use WPA2

Wi-Fi Protected Access2, or WPA2, is one of the strongest and most complex security algorithms available for safeguarding your Wi-Fi network.

Implement a VPN

Virtual Private Networks, or VPNs, are essential for remote workers, since they reduce the risk of information being intercepted as it travels between networks. VPNs will help protect home workers from accidentally using vulnerable public networks.

Build your firewalls

It may seem obvious, but strong firewalls are still one of the most effective cybersecurity weapons in your arsenal. Make sure you have an internal firewall as well as an external one and look at layering hardware and software-based firewalls and make sure they are updated regularly for the greatest protection.

Disable file sharing

Although collaboration is fundamental for remote workforces, file sharing presents a real opportunity for hackers to access sensitive information or cause damage to your systems. Implementing cloud-based or password protected systems will enable collaboration without leaving your network vulnerable.

Secure your endpoints

Especially printers. Printers and other plug-in equipment like scanners and portable hard drives are often overlooked when it comes to network security. Make sure their software is up-to-date and consider Secure Print – a feature that allows users to delay the actual printing until they are physically in front of the printer.

Printer security

One area of network endpoint risk that often gets overlooked is printer security. Printers often appear to be fairly safe devices, but they can be used by hackers as a backdoor into your network. And this happens more often than you might expect.

More than one in 10 security incidents that affect a business involve a printer.[14]

That's because most modern printers are connected to the internet, and this network connection runs two ways - from your device to your printer, but also from your printer back to your device. And while users don't think twice about printing out sensitive information, this two-way connection can be exploited by smart hackers if your printer doesn't have defences that are as robust as your computer.

According to Brother research, 95% of all organisations are concerned with ensuring network security for their hybrid workers.

Security by Brother is our solutions-based approach to endpoint security that makes business printing secure. We introduce triple-layered security at a network, device and document level to ensure that your information is only ever seen by those it's meant for.

[14]Quocirca.

And so to finish...

We've found that a "must have" and "nice to have" approach to risk reduction is the best way to make sure that ITDM's budgets are spent effectively. We can break these down into:

Non-negotiables: elements that are essential for success, such as a configured firewall, antivirus software, VPNs, basic cybersecurity training and password managers.

Added value: elements that would be beneficial, but aren't essential to provide a basic level of cybersecurity, such as multi-factor authentication and regular training sessions.

After identifying your organisation's biggest risks, this method enables you to determine which security measures are crucial for keeping your organisation safe, and which could be extremely beneficial if you've got the budget. This method is also a great way for ITDMs to get additional budget for their defences.

Ultimately, cybersecurity isn't just another list in a checkbox exercise of routine training for the people in your organisation. To keep your systems and data safe, cybersecurity needs to become a way of life among your teams – with spotting cyber risks as natural as spotting road risks while driving.

Know the threats

Contact your Brother security expert today.

brother
at your side

in[ctrl]

In partnership with KnowBe4
Human error. Conquered.