brother
at your side

The print security blind spot

IT professionals are underestimating print security risk – we speak to cybersecurity experts about the threats that businesses face

Contents

Rising to the challenge

Andy Johnson

Head of product and solutions management, Brother UK

We are living in a golden era for cybercrime. Barely a day goes by without a major incident and more UK firms are reporting attacks than ever before[i].

Are IT professionals adequately prepared? What can they do to mitigate critical risks? It seems that vigilance isn't the watchword in every area.

The stakes have never been higher when it comes to protecting companies from data theft and ransom demands. But while this issue is clearly a priority for IT professionals, the role printers play in a network's security is often overlooked, despite them being an integral part of nearly every company's infrastructure.

More than one in ten[ii] of all security incidents that affect businesses involve a printer, 59 per cent of which result in data being lost. Importantly, the threat is no longer the preserve of large companies as hackers shift their focus to supply chains and smaller businesses which might be easier targets.

But according to our research, only a quarter of IT professionals are looking to invest in print security, while far more (46 per cent) are only concerned with cutting costs.

Three quarters say they have never invested in document encryption and 56 per cent are not using user authentication.

There is a significant blind spot here and it's clear that many are underestimating the risks they face. In this report, we speak to four leading lights in the UK's cybersecurity industry for their insight on how to tackle this issue, how black-hats target printers and the strategies IT professionals can put in place to secure their networks.

As you read on, you'll discover that many of these demand more than the extensive technical expertise of IT professionals – most are people-focused and require behavioural change within the business.

I hope that this report will go some way in helping promote a better understanding of the vulnerabilities printers can open companies to and encourage the adoption of strategies that will enhance security.

> "More than **one in ten**[ii] of all security incidents that affect businesses **involve a printer**, 59 per cent of which result in data being lost."
>
> **Andy Johnson, Brother UK**

i https://www.hiscox.co.uk/sites/uk/files/documents/2019-04/Hiscox_Cyber_Readiness_Report_2019.PDF
ii Quocirca Global Print Security Landscape 2019 https://quocirca.com/wp-content/uploads/2019/02/Quocirca-Print-Security-Feb-2019-Final-Web.pdf

The threat

A golden era for cybercriminals

Every organisation is a potential target for cybercrime, and for those that fall victim, the impact can be significant. The scale is difficult to quantify, but it is a growing and rapidly evolving danger that no business can afford to overlook.

Vince Warrington, CEO of cybersecurity specialist Protective Intelligence, said: "This is the golden era for cybercriminals.

"The threat doesn't come from kids in their bedrooms messing about with computers any more. Most of what we see is proper organised crime operating on a vast scale.

"We're even hearing about drug cartels moving into cybercrime because it's much more profitable, and they are less likely to get caught because law enforcement is still behind the curve."

It's not just multinational corporates that need to fear being the subject of targeted attacks - SMEs are now just as much under threat. In fact, there is evidence that these companies are less likely to have anti-cybercrime precautions and protocols in place than is the case with bigger enterprises, representing a significant security blind spot.

Changing tactics – from theft to extortion

In times gone by, cybercrooks' tactics were to steal things like credit card data, which could then be sold on the dark web, hidden parts of the internet that are encrypted and can't be found using traditional search engines.

So successful was this strategy that the web was flooded with such data and its value was decimated.

Now the focus has switched to ransomware, malicious software designed to deny access to a computer system or data until a ransom is paid.

9,741

cyberattacks on British SMEs every day[i]

£25,700

average cost to business of a cyberattack[ii]

i www.fsb.org.uk/media-centre/press-releases/small-firms-suffer-close-to-10-000-cyber-attacks-daily
ii https://www.hiscox.co.uk/business-insurance/cyber-and-data-insurance/faq/small-business-guide-to-cyber-attacks

Less sophisticated crooks might use a scattergun approach, infecting as many computers as possible and demanding relatively small amounts of money – perhaps £150 to £250 – to unlock them.

But more advanced attackers will do their homework on an organisation and specifically target its most valuable assets. With their target paralysed and unable to function, they can then extort huge amounts of money, potentially well into six figures.

Even if companies don't pay up, the costs of a clean-up or coping with infected systems can be huge. In June 2019, it was reported that global aluminium producer Norsk Hydro had lost £45m as 35,000 employees were forced to switch to pen and paper and production lines reverted to manual functions following a ransomware attack.

The printer blind-spot – the first point of entry into an organisation

While businesses are increasingly waking up to the threat of cybercrime, there remains a significant area which our research reveals is being overlooked by the majority of companies - print systems.

Criminals have begun to target printers, as well as other connected devices, even vending machines, as they are now increasingly sophisticated with greater functionality.

Colin Robbins, managing security consultant at cybersecurity specialist Nexor, said: "Modern printers are essentially computers that produce paper, so there are ways to take over the printer and use that as the first point of entry into an organisation.

"The reason printers are particularly vulnerable is because most now have value-added services like the ability to receive print jobs by email. If a printer has a direct communication channel with the internet, then it's a potential route into an organisation."

But there are strategies that IT managers can adopt to ensure their systems are robust and in the following pages you'll learn from some of the UK's leading cybersecurity experts.

It's an issue that requires a joined-up approach, with both technical and cultural aspects, but the consequences of not protecting yourself effectively are so potentially damaging that it is something no business can afford to overlook.

> "This is the **golden era for cyber criminals.** Most of what we see is proper organised crime operating on a vast scale."
>
> **Vince Warrington, Protective Intelligence**

Meet the experts

Colin Robbins
Managing security consultant, Nexor

Colin spearheads Nexor's security consulting capability, providing advice and guidance to external customers and internal projects. Nexor specialises in helping customers maintain effective defences against persistent and evolving threats.

Gemma Moore
Director, Cyberis

Gemma is one of the most qualified penetration testers in the UK, according to CREST, the international not-for-profit accreditation and certification body. Cyberis is a leading consultancy with a specialist incident response team that manages security incidents from initial detection to closure.

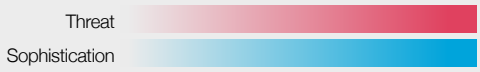
Andrew Barratt
UK managing director, Coalfire

Andrew has almost 20 years' experience working in IT infrastructure, information security and assurance services across the world for both government organisations and the private sector. Coalfire is an international cybersecurity agency headquartered in Denver, USA, providing risk management and compliance services for enterprises and government organisations.

Vince Warrington
CEO, Protective Intelligence

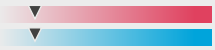
Vince has more than 15 years' experience heading large-scale, organisation-wide IT and cybersecurity programmes for central government departments, blue chip companies and well-known voluntary organisations across the globe. Protective Intelligence advises public and private-sector organisations of all sizes on the best ways to navigate the ever-changing information-security landscape.

Meet the cybercriminals



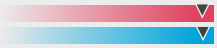
Colin Robbins, managing security consultant at Nexor, identifies the cybercriminals who could be targeting your organisation.

Bedroom hacker



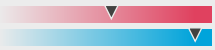
Often working alone, the bedroom hackers are a relatively low threat and not particularly sophisticated. They're opportunists who look for easy targets and take what they can.

Organised crime



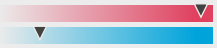
Better resourced, more sophisticated and often operating beyond the reach of law enforcement. They know what they are looking for and how they can turn that into money. They could use ransomware, steal data to sell or target sensitive information that can be used for insider dealing.

Secret agents



Employed by nation states, they will use businesses as a way of getting to intelligence they want, perhaps about potential targets like national infrastructure and energy supplies.

Disgruntled employees



Internal threats tend to come from disgruntled employees who have been overlooked for a promotion or have some gripe against the organisation.

Securing devices and user access

The work to ensure your printer is secure starts the moment you take it out of the box.

The sophistication of modern printers, including the ability to email print jobs and connect wirelessly, brings huge convenience and flexibility. But this functionality can also present a security risk unless it is managed effectively.

Most modern, networked printers run a full operating system, are handling sensitive data and often have a trusted relationship with the internal network.

However, they are not necessarily treated in the same way as assets like workstations and servers, and patches and updates individual users need to make on their machines are often ignored.

An unprotected printer that is connected to an organisation's network can be discoverable using Internet of Things search engines like Shodan or Censys, allowing an attacker to use the machine's functions, modify its settings or even change the password, denying the owner access.

IT managers can take straightforward steps to avoid these risks, which include keeping on top of password management, never leaving default options in place and always installing firmware upgrades as soon as they become available.

Hard to detect

Colin Robbins said: "As an attacker, if I can take control of your printer, I'm then effectively in control of a computer that's inside your organisation.

"That gives me a great launch point for other attacks. I can either use network attacks or what we're increasingly seeing is the printer being used to send phishing-type emails.

"Because they originate from inside the organisation, they look much more genuine and are much harder to detect."

Secure set-up

According to Gemma Moore, in many cases the deployment process for new hardware is to blame for exposing a system to risk.

"The more functionality your printer has, the greater its attack surface area and the greater the amount of risk management you need to do when installing one" she said.

"But manufacturer default settings tend not to get changed, particularly in smaller organisations. Where default passwords are left in place, and free access to all functions is granted to all users, these functions can be open to abuse.

"Larger businesses and government departments often have a process for deploying a printer, but smaller organisations don't."

The advice is simple: when you buy a printer, make sure you control user access to its more advanced functions, change any default passwords and switch on any secure capabilities.

Outmoded IT

Some printers represent a significant investment for businesses and many organisations still use legacy equipment that was designed and built before security awareness was as heightened as it is today.

Vince Warrington said: "You need to know about the vulnerabilities of your devices. An older printer might have an administrator password that is hard-wired into it, is widely known on the internet and cannot be changed.

"If you have older printers that you know are vulnerable and are being used for printing confidential documents, why not replace them with devices that you know have better security?

"It's down to IT departments to ensure organisations are as secure as they can be."

Andrew Barratt echoed this message: "Anyone that uses the phrase 'it's just a printer' is doing things wrong. Now that the devices are so sophisticated, it's critical that we move away from that kind of thinking and ensure printers are given just as much consideration when it comes to security as any other part of the network."

> "Anyone that uses the phrase **'it's just a printer'** is doing things wrong. Now that the devices are so sophisticated, it's critical that we **move away from that kind of thinking.**"
>
> **Andrew Barratt, Coalfire**

Document management

Securing assets against cyberattacks

Even the seemingly value-less documents that businesses use as part of their standard operations can be useful to cybercriminals when it comes to committing fraud, so keeping this documentation safe from creation to deletion is vital.

Andrew Barratt said: “I think a lot of business managers would be amazed if they knew how useful even apparently innocuous documents can be to a criminal.

“Invoices are a particular concern. Some of the most common crimes we see involve impersonating an individual that works for a business and requesting a payment be made using fraudulent bank details.”

Often, by the time the fraud has been discovered, the payment has been processed and the money is gone.

Presenting a convincing impersonation of the company the criminal is pretending to represent is a key part of these scams, and the ability to gain unauthorised access to genuine documents so they can be copied is a vital stage in their process.

With that in mind, it’s essential for businesses to be aware of – and to have considered – where and how documents are stored.

Andrew Barratt continued: “Far too often we find that’s not the case, and printers are a major culprit because they can form an unsecured output point in the network. We frequently see older printers that have default ‘admin 1234’-style login details that haven’t been updated, and these provide an open goal to criminals looking to get into the system and gain access to documents that should be restricted.”

> “If you went to a printer recycling centre, I guarantee you’d find a lot of data that could be very useful to a hacker.”
>
> **Andrew Barratt, Coalfire**

End-to-end protection

Network-connected printers are a standard feature in businesses around the UK, with large numbers of employees often sharing access to a device located in a shared space that's accessible to all.

While this is a convenient and efficient way to organise print infrastructure, it can also create vulnerabilities.

Gemma Moore said: "Many printers implement file transfer protocols (such as FTP or SMB) to allow batch printing. But these systems are often not as secure as they should be, with weak password protection, storing unencrypted documents and not deleting them in a timely way.

"You can end up with a big queue of potentially sensitive documents sitting in the printer's internal storage, easily accessible not just to anyone with physical access, but potentially to any external hackers that might have found a way into the network."

The information stored inside printers can also create issues when it comes to disposing of older hardware.

Andrew Barratt said: "If you went to a recycling centre and retrieved the discs from the business-grade printers there, I guarantee you'd find a lot of data that could be very useful to a hacker.

"Even if the data is several years old, in many cases it can still tell you a lot about the people inside an organisation, their roles and relationships – potentially a gold-mine for the kind of intelligence cybercriminals are looking for."

Keeping documents secure

All of this underlines the importance of treating the data sent to printers with the same level of attention it is given at every other stage. Documents should be encrypted, right up to the moment they become a hard copy.

Those print-outs should then be protected by ensuring that nobody except for the person that sent them to print is able to retrieve them. This can be done using access cards with near-field-communication (NFC) technology, or simply by giving each user their own password.

The effectiveness of passwords can be improved by allowing users to use the same sign-in that gives them access to other parts of the network. This way, it will automatically update whenever their main password is changed, reducing the likelihood of easily-guessed default log-ins being used.

Documents can be just as vulnerable in hard-copy if genuine supplies for things like toners and cartridges aren't used.

Some 'compatible' supplies can store impressions of potentially sensitive data creating unnecessary vulnerabilities, especially in cases where very sensitive documents are being printed

Finally, at the end of a printer's life, businesses should ensure that all data on the outgoing unit is deleted by wiping internal storage. This can often be done digitally, but in some cases may mean the physical storage needs to be destroyed. It's worth checking with your print supplier if this is a service they offer.

> **Documents are often not as well secured as they should be,** with weak password protection, storing unencrypted documents and not deleting them in a timely way.
>
> **Gemma Moore, Cyberis**

Management processes

Embedding security in c-suite strategy

Cybersecurity should be high on the agenda of everyone in an organisation, but it's important that management have oversight of a joined-up strategy.

We've seen how the threat from cybercriminals is constantly evolving and changing.

In response, printer manufacturers monitor the threat and issue regular firmware updates to address new security issues that come to light.

So, schedule regular checks to ensure printers are using the latest and most secure firmware updates.

Colin Robbins said: "A device like a Windows computer will tend to update itself when it needs to.

"Although most devices are automatic too it's best practice to put it on a calendar schedule that once every three months you check if there are any updates that need to be applied."

Legacy hardware

But firmware updates are only issued for printers that are part of a manufacturer's current product range and, once a model is discontinued, updates end and it can quickly become vulnerable. A well-made printer can feasibly outlast its support lifecycle, so it's vital to maintain a network of modern devices that are protected against the latest cyberthreat.

Signing up to a Managed Print Service (MPS) including hardware is an effective way of ensuring printers are up-to-date, efficient and secure, and an MPS often comes with an initial print assessment which can identify print and IP security risks your organisation faces.

The subsequent MPS programme should help mitigate those risks with a tailored print security plan.

Spotting unusual activity

IT managers should also employ Security Event and Incident Management tools to identify potential security events.

These monitoring systems can alert IT teams to unexpected activity that could pose a threat.

Vince Warrington said: "There are various tools that you can use, some of them are even free nowadays, which are really good at pointing out unusual activity that's happening on your network.

"For example, you'd expect your printers to be used between nine and five in a normal office environment, but if you suddenly find somebody's accessing that printer in the early hours then that's worth investigating."

Getting the basics right

When it comes to ensuring management processes are in line with best practice, the experts we spoke to for this report backed an initiative by the National Cyber Security Centre called Cyber Essentials, which helps guard against the most common cyber threats.

It includes five technical controls that can help you to protect your organisation against a whole range of the most common cyberattacks.

They are:

1. secure your internet connection
2. secure your devices and software
3. control access to your data and services
4. protect from viruses and other malware
5. keep your devices and software up to date

Colin Robbins added: "If you're going to do anything on security then do these five things and do them well and you will stop the majority of attacks."

Only human

The weakest link in any security strategy is often human, so organisations shouldn't rely on technology alone to address cyber-risk.

Rather, they should foster a culture where all colleagues understand that they have a responsibility and a role to play in protecting data.

Vince Warrington said: "There's lots of end-user training available, but most people don't retain what was on the course really well, so we advocate an everyday approach.

"For example, if there's a high-profile cyberattack on a business, message everyone to remind them not to open attachments from unknown sources.

"It's about making security part of everyday office life so it's always on colleagues' minds."

> "It's about making security part of **everyday office life** so it's always at the back of colleagues' minds - or even the front of their minds!"
>
> **Vince Warrington, Protective Intelligence**

Five key takeaways to step up your print security

Protecting your printers and removing the vulnerabilities most commonly targeted by criminals doesn't need to be a complex or time-consuming task. In fact, following these five simple rules will help protect your business against most printer-related cyberattacks and data breaches.

1. Treat your printer like the rest of your network

Think of your printers in the same way you would servers or workstations. Do all of the same things you would for those things, including carefully configuring them to change default settings and regularly installing update patches.

Look for a printer vendor that is able to give you guidance on securing your printers and be sure to follow their advice.

2. Ensure robust user access control

Think carefully about user access and put appropriate controls in place. More advanced functions should only be accessible to trusted individuals, and everything should be password-protected.

Brother's Secure Print+ solution offers easy-to-manage card-based user authentication that ensures documents are only printed when they're ready to collect them from the printer, avoiding sensitive documents falling into the wrong hands.

3. Regularly update firmware and hardware

Keep your hardware up-to-date. There is an arms-race between cybercriminals and software developers working to keep your data safe and neglecting to install driver and firmware updates can make you a target. If your printers are too old to accept updates, it's probably time to upgrade to a more secure option.

Brother regularly issues updates to ensure its products remain at the forefront of printer security, and a step ahead of hackers.

4. Build-in end-to-end encryption

Ensure that data is encrypted right up to the moment the ink or toner touches the paper. This will avoid the risk of data being intercepted either while en-route from the network or while stored on the printer itself.

All Brother networked printers feature end-to-end encryption. Always ensure this feature is enabled and if in doubt, contact Brother or ask your printer vendor for guidance.

5. Always use secure consumables

Be sure to use consumables, such as toners and cartridges, that come with a data security guarantee. Imitation supplies can accumulate impressions of previous print jobs and reprint them onto new documents.

Brother's Genuine supplies have been tested by independent authority Smithers PIRA, based on known methods used by criminals, to guarantee your data is protected.

Tackling the blind spot

Andy Johnson
Head of product and solutions management, Brother UK

From the disgruntled employee to the organised criminal gang, the number of possible attackers is growing and the threat of a cyberattack is no longer confined to large corporates with vast amounts of customer data.

It's a risk that every company must now be alive to and as we've explained in this report, your printers cannot be overlooked. They have a trusted relationship with the rest of your internal networks and need to be treated in the same way that you manage your other assets.

It's understandable that finding new efficiencies should be a focus as businesses look to streamline their operations to do more for less. But that should not come at the expense of ensuring you have a secure printer network.

This doesn't require significant investments in new technology either. As the experts interviewed for this report explain, many of the vulnerabilities require cultural and behavioural changes. Whether that's ensuring documents are encrypted, right up to the moment they become a hard copy or using the latest firmware updates and disposing of old devices correctly.

We understand the challenges that businesses face – from productivity through to ensuring they have secure print and scan devices – and are here to help.

We work with our customers to keep their print network up-to-date, efficient and secure through our Managed Print Service (MPS) and all of our products include end-to-end encryption and port-based access control, designed to allow you to connect and share documents in confidence.

I'd like to thank our experts for contributing their thoughts to this report and supporting us in highlighting the vulnerabilities that businesses face as well as the opportunities there are to improve security. I hope that reading this has provided you with information and understanding you need to enhance your network security.

> "We **understand the challenges** that businesses face - from productivity through to ensuring they have secure print and scan devices - and are **here to help.**"
>
> **Andy Johnson, Brother UK**

Useful contacts

Matthew Jones
Head of end user sales
matthew.jones@brother-uk.com
07786 561029

Jessica Stansfield
Senior client manager
jessica.stansfield@brother-uk.com
07769 155942

Richard Titmuss
Senior client manager
richard.titmuss@brother-uk.com
07867 970583

Stephen Moore
Senior client manager
stephen.moore@brother-uk.com
07769 586395

brother
at your side

www.brother.co.uk

Brother UK Ltd.
Shepley Street, Audenshaw
Manchester, M34 5JD

Email: enquiries@brother-uk.com

Tel: +44 (0) 333 777 4444