HYBRID BUSINESS NOW

Information Security in the Hybrid Workspace

MAKE IT
HERE
SECURE
TOGETHER

Canon

FOREWORD

Paul Colwell, Chief Technology Officer at Wavenet

The pandemic may be over, but its lasting effect on the way businesses operate, and the way we work remains evident. Organisations who previously hosted applications on site with employees travelling into offices for access, had to quickly find alternative ways of working in the early days of lockdown.

IT teams should be commended for their work setting up employees for remote operations in such a short time. However, in this rush to remotely keep businesses running, compromises had to be made and security measures were often overlooked or implemented incorrectly.

The damage done by taking these shortcuts and not applying the same standard of security implemented within a physical office, needs to be repaired. Hybrid working has increasingly become the norm in the wake of the pandemic and this remarkable transition. The resulting borderless networks and migration to cloud-based systems like Microsoft 365 means information sharing has increased, which in turn has provided increased ways that security can be compromised. Uncontrolled and unsecure employee-owned devices, open home Wi-Fi networks, weak passwords, rushed compliance practices and unencrypted file sharing carry extensive risk for a business.

It's much harder nowadays to detect criminal activity across a network, especially when not in a secure, closed office environment. Hybrid working has made the boundary of an organisation's network ambiguous and difficult to distinguish between what should and shouldn't be there. This means the security of each endpoint – laptop, server, printer, or phone, has become ever more important.

MOVE WITH THE TIMES...

Now is the time to consider implementing practices like effective network segmentation. By dividing up the internal network, an organisation can appoint more protection and controls around key assets. Movement around the network can be restricted so that employees who don't need access to certain areas can't do so, and neither can cyber-criminals.

The monitoring of laptops, systems, and other collaboration tools, need to be improved by implementing strategies that can quickly identify possible compromises, respond effectively, and recover from any breach. The lifecycle of this technology must also be considered. Each device should be patched with the latest updates, and then at end of life, the device needs to be disposed of properly as sensitive information can still be hacked if care is not taken.

This better understanding and greater control over who is looking at what is vital. Solutions are available now that allow businesses to set automated policies around access, editing, and sharing of information. By implementing such a solution, an organisation can maintain control of critical and sensitive data, reducing the chance of data leaking, whether deliberate or accidental.

EMPLOYEE APPROACH...

Employees and the way they behave outside of a secure office, must also be considered. Collaboration tools for employees to communicate and share information across networks are essential to a hybrid workforce. This means it's not uncommon for sensitive business conversations to happen on a mobile phone, Microsoft Teams and Zoom, or confidential documents sent via Dropbox that cyber-criminals are keen to exploit. Meetings are often held in cafes and other public spaces which means public Wi-Fi hotspots need to be considered as well.

With colleague advice no longer a desk away, hostile approaches by cyber-criminals via email and on platforms like WhatsApp and LinkedIn, are on the rise. Malicious interception of emails, altering contact information and deceiving recipients into divulging information are all cyber-criminal strategies. If a mobile device is compromised by an employee clicking on a phishing link, or sharing a password or PIN, the whole network could then be compromised.

This is why a security-first culture needs to be promoted and deployed. Employees need to be educated so they're aware of potential risks and implications. They should know the value of using a password manager and multi-factor authentication for both personal and professional account logins and advised not to click on links or give away information to unexpected contacts.

To repair the damage created during the pandemic, remote information security going forward in this hybrid working era, requires every employee to change their mindset, adopt new approaches and be continuously reminded about workplace security and the latest company policies. The right set of people combined with the right processes and technology will allow for the deliverance of strong cyber security and improved resilience to an organisation.

Wavenet are experts in cyber security and risk mitigation. With an extensive knowledge and vast experience in protecting critical assets from the ever-changing threat landscape, Wavenet can help organisations assess, develop and manage their cyber resilience.

THE WORLD HAS CHANGED – AND INFORMATION SECURITY HAS CHANGED WITH IT

Successful hybrid working depends heavily on collaboration tools for employees to communicate and share information across networks. While these tools are essential to the hybrid workforce, they can also be a critical point of vulnerability – which cybercriminals are keen to exploit.

And, indeed, they have. Remote workers were easy targets for hackers in the early days of the pandemic, because they would often be using unfamiliar systems and unknowingly make themselves vulnerable to cyberattacks. At the same time, organisations cut their spending on security as part of overall budget tightening, thus reducing their cyber resilience.[1] All of this happened against the backdrop of a longer-term increased focus on data protection, long before Covid-19 became a household name.

Changes in data protection regulations mean that businesses must take more control of how they collect, process and store company and personal data. This includes data residing in printers and multifunctional devices. Those that don't comply with such regulations can face fines up to 4% of their annual global turnover or €20 million (whichever is greater) under the EU's GDPR regulations.[2] The UK's Data Protection Act 2018 comes with equivalent fiscal penalties.

But beyond the financial risks posed by cybersecurity threats is the potential for significant reputational damage. This is just as – if not more – destructive for day-to-day business. Case in point: software company SolarWinds was the subject of a massive cybersecurity attack in early 2020 that spread to the company's clients.[3] Major firms like Microsoft and top government agencies were attacked, and sensitive data was exposed, resulting in $3 million in fines and lasting reputational consequences.[4]

That was then, this is now.

The workplace has evolved so much since the early days of the pandemic that it's even harder to keep these threats at bay. As you continue to develop hybrid working plans, it's more important than ever to prioritise robust security.

[1] https://www.computerweekly.com/news/252484783/Coronavirus-Cyber-security-spend-to-slow-in-2020
[2] https://www.itgovernance.co.uk/dpa-and-gdpr-penalties
[3] https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?r=US&IR=T
[4] https://www.jdsupra.com/legalnews/the-solarwinds-cyber-attack-the-6179862/

You don’t generally hear about the information security successes. Some businesses are lucky, others are vigilant - and there are certain behaviours that unite those businesses. This eBook looks at those specific behaviours and how to manifest them within your organisation, starting with **three key focus areas every leader and IT decision maker should consider first.**

1 INFORMATION SECURITY STARTS WITH YOUR PEOPLE

Cyber-attacks in the early days of the pandemic often took advantage of employees’ unfamiliarity with new communications platforms – like video conferencing – and the general uncertainty of the time.[5]

The 2020 Verizon Business Data Breach Investigations Report highlights a significant scaling up of cyber threats across the board with credential theft and social attacks such as phishing and business email constituting the cause of over 67% of all breaches.[6] According to the report, 82% of all data breaches involved ‘the human element, including social attacks, errors and misuse. Your workforce may now be more confident using teleworking tools, and your IT team more prepared, but the potential for cyber-attacks and data breaches is still very real.[7]

What’s more, employees themselves may not be using the most secure means of sharing information. ‘Shadow IT’ is the use of IT systems – software, devices like printers and scanners, apps and file storage – that have not been provided or approved by an employer but used by staff because they find them more familiar or easier to use. It’s typically done for reasons of convenience and efficiency rather than with malicious intentions, but can present a serious problem.

Not only are consumer-grade, off-the-shelf systems less secure than those developed for business use, but if IT teams haven’t approved them, they can’t oversee their security – leaving another door open to attackers. According to our 2022 research, one in five employees still have to provide their own equipment. And the same proportion of employees struggle to get remote IT support.

Alongside the need for IT standardisation and support, there’s a crucial behavioural element to consider: it takes time for people to establish new habits and learn new ways of working. 77% of IT teams report that employees stop following security procedures when offsite.

Moreover, when the boundaries between work and home blur, so do barriers to business-critical data. Even the experts can become lax: in a poll of IT security personnel in North America and Europe, 20% admitted to allowing members of their households to use work devices during lockdown.[8] Children doing schoolwork or partners browsing YouTube may seem innocent enough, but it only takes a click of a mouse by an untrained person to allow a hacker into an organisation’s security perimeter.

77% OF IT TEAMS REPORT THAT EMPLOYEES STOP FOLLOWING SECURITY PROCEDURES WHEN OFFSITE.

When laptops, phones and shared printers without adequate security provisions are used in public – in airport lounges, libraries, even professionally managed co-working spaces – there is the additional risk of strangers grabbing the opportunity of data theft. **You never know who’s looking over your shoulder.**

Similarly, people working on-the-go could compromise data security by connecting an improperly secured laptop or phone to a public network. If a cyber attacker spots these entry points, it not only affects the smooth running of a company day-to-day but can also have serious long-term repercussions.

Even organisations with a fully on-site workforce should be aware of their place within a supply chain where other businesses may have adopted remote or hybrid working. In addition, moving to the cloud can render traditional network security frameworks obsolete. But security moves as quickly as criminal activity, with modern services like Zero Trust providing continual resilience.

But these dangers can also be reduced through education. As an employer, it’s essential to provide security and compliance guidelines and employee training on how to uphold them. Security should be an ongoing investment and priority – rather than an ad hoc approach – in order to give an organisation the confidence to make decisions and move forward.

ZERO TRUST, A SECURITY FRAMEWORK THAT REQUIRES ALL USERS TO BE AUTHENTICATED, AUTHORISED AND CONTINUOUSLY VALIDATED, IS A CONCEPT CREATED SPECIFICALLY FOR THE HYBRID WORLD.[9] WHEREAS TRADITIONAL SECURITY PROCEDURES TYPICALLY ONLY REQUIRE A VALID LOGIN ID AND PASSWORD TO GAIN ACCESS TO A NETWORK, THE ZERO TRUST APPROACH USES SEVERAL CHECKS BEFORE A PERSON (OR DEVICE) IS GIVEN ACCESS.

[5] https://www.theguardian.com/technology/2020/may/24/hacking-attacks-on-home-workers-see-huge-rise-during-lockdown
[6] https://www.verizon.com/business/resources/reports/dbir/
[7] https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-april-2022-14-3-million-records-breached
[8] https://www.securitymagazine.com/articles/94997-it-security-professionals-demonstrate-excessive-trust-despite-concerns-with-remote-work-security-programs
[9] https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/

# 2 INFORMATION SECURITY CONTINUES WITH YOUR DEVICES

Printers, scanners and any number of gadgets within the realm of the Internet of Things can present unlocked doors to hackers who know how and where to look for them. Within a trusted network, like that typically used in a company office, the ability to access devices remotely offers numerous benefits. However sometimes – often inadvertently – equipment like home printers can be connected to untrusted networks, and even directly to the internet, without passwords or firewalls.[10]

Modern multi-functional printers are **endpoint devices** and are just as powerful as a PC.
As a result, it's possible for printer firmware to be targeted by hackers attempting to gain access to the network and corporate data. An attacker could make changes to email directories so a document can be sent to a recipient outside the organisation. Or they could intercept a document transmitted over HTTPS if the document and its data are not encrypted.

WHAT'S AN ENDPOINT?

AN ENDPOINT IS ANY DEVICE THAT CONNECTS TO THE CORPORATE NETWORK FROM OUTSIDE ITS FIREWALL, SUCH AS LAPTOPS, TABLETS, MOBILE DEVICES, POINT-OF-SALE SYSTEMS AND, OF COURSE, DIGITAL PRINTERS.

PRINTJACK:
THE PRINT INDUSTRY'S WATERGATE SCANDAL

At the end of 2021, a team of Italian researchers published a report exposing 50,000 printers in Europe that were vulnerable to remote, virtual attack. They identified three types of 'Printjack attack'.[11]

The first, a kind of recruitment process, involves exploiting a network loophole to infect printers with minor bugs, causing them to overwork and decay over time. The second is more serious. A 'paper DoS attack' forces devices to print repeated jobs until they run out of paper, causing significant disruption in the workplace. The third and most profound is a Man-in-the-Middle breach, whereby hackers access all printed data while remaining invisible themselves.

All three types of 'Printjack' were possible because of vulnerabilities in the devices' network connections. But, with strict authentication protocols and a solid security framework, they can be avoided.

Indeed, the researchers found rampant non-compliance with GDPR and ISO/IEC 27005: 2018 across Europe. And of the 50,000 printers they exposed, the majority were in Germany, Russia, France, Netherlands and the UK.

And security measures shouldn't stop with the devices that your teams are actively using. Have you thought about those old, dusty laptops, hard drives and printers that are locked in some storage room? What about them?

Data stored in workplace devices is often overlooked, but the reality is that the security risks don't end when you stop using a device and lock it away. It's far from out of sight, out of mind. When these reach their end-of-life, anything less than in-depth, professional data removal poses a real threat.

Consider a printer that's been sitting in that back-office storage room for years, perhaps even for decades. Despite never being used, it's still working and connected to the Internet. Unintentional backdoors like these are just another route in for savvy hackers, especially when workers are generally aware of their existence.

In short, strong and robust security means having visibility over the full lifecycle of the devices in use – protecting them throughout their operational lifetime, including end-of-life.

And hybrid working imposes new challenges when a portion of your device fleet is sat in employees' homes. Our research shows that 73% of IT decision makers are unable to safely dispose of data from off-site printers and scanners. It's essential, then, to have an exhaustively comprehensive view of the entire lifecycle of your devices.

This starts with making sure everything that's plugged in is actively monitored and updated with the latest security patches. When disposing of old devices, follow a pre-defined procedure, from securely erasing all data, disconnecting devices and properly destroying any hard disks to running a complete audit – which should include a detailed check to remove any residual physical information from devices, USB slots, media trays, and so on.

You can never be too careful. Nowhere is this truer than in the case of data disposal, where it's not enough to simply follow these steps. It's just as important to keep accurate records should you ever be prompted by an official body to provide evidence.

[10] Canon Research, 2022
[11] https://arxiv.org/abs/2111.10645

3 COMBINING BEST PRACTICES AND SMART TECHNOLOGY POLICIES

It's common, particularly early in the adoption of a hybrid working model, for workers to use devices that may not have been company-supplied or approved. It's also harder for IT teams to ensure these devices are properly set up, they receive the updates they need and that the data they contain is safely managed.

Providing training and guidelines to employees, while important, is unlikely to be enough to mitigate or avoid all information security challenges. Selecting the right technology processes and protocols can help circumvent information security issues caused by human error.

WHAT PHYSICAL RESTRICTIONS COULD YOUR IT TEAM IMPOSE?

There are tools on multi-functional printers to prevent people accessing documents they shouldn't, such as PINs, ID cards and permissions based on role, department, seniority and more. These tools provide reassurance that information kept on-site won't fall into the wrong hands.

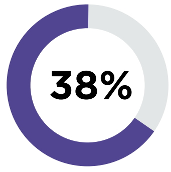
Something else to consider is email monitoring software. This exists to circumvent human curiosity when it comes to opening emails from unknown senders, and does so without infringing on workers' rights to privacy – which should never fall by the wayside, even in high-risk times like these.

BUT WHAT ABOUT THE DATA THAT LEAVES THE OFFICE?

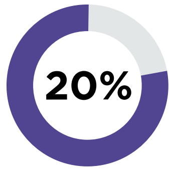
All hybrid organisations should enforce rules around any portable, information-carrying devices, including laptops, work phones and, most importantly, USB drives. Also, disallowing downloads and installations to company hardware without permission is highly recommended.

> **"MORE THAN A QUARTER (27%) OF ORGANISATIONS TOLD US THAT THEY HAD EXPERIENCED BUDGET CUTS THAT AFFECTED THEIR SPENDING ON CYBER RESILIENCE IN 2020."[13]**

In a poll of IT security practitioners across North America and Europe, 38% said data control during the pandemic has been very hard to manage. Nearly 20% said their work devices were used by other members of their household.[14]



said data control during the pandemic has been very hard to manage



said their work devices were used by other members of their household

ORGANISATION X SUFFERED A MAN-IN-THE-MIDDLE BREACH, AN ALMOST INVISIBLE ATTACK.[12]

ATTACK

Adversaries attacked Organisation X client portal. By redirecting the portal's traffic to their own system, they were able to access all incoming and outgoing client communications. These were experienced hackers, as evidenced by their infrastructure's seamless integration with the portal log-in page.

RESPONSE

When Organisation X realised the files had been compromised, they contacted the affected customers immediately. They then formed two damage control teams: a technical, investigative team and a crisis team who advised the board.

TAKEAWAYS

Act fast, ensuring that your risk appetite is aligned with any third-party organisation's security. Also, employ proper security controls in the areas of prevention, detection and response.

> **"BY RESPONDING SO QUICKLY WE WERE ABLE TO REALLY LIMIT THE IMPACT."**
> ***– ORGANISATION X***

[12] *https://www.youtube.com/watch?v=ZpGZEoYv8Ts*
[13] *NCC Group's Insight Space report, Paying off the cyber debt: How are decision makers approaching cyber resilience in 2021?*
[14] *https://www.securitymagazine.com/articles/94997-it-security-professionals-demonstrate-excessive-trust-despite-concerns-with-remote-work-security-programs*

NEW WORKING MODELS, NEW SECURITY CHALLENGES

Security and compliance should be central to the planning of any future business operating model. Whether it's software platforms, hardware or governance, your organisation needs to continually review your security strategy to ensure it's ready to deal with the changing threat landscape fostered by hybrid working.

Many organisations are already taking action: 48% of IT decision-makers polled in a European survey plan to make cyber security infrastructure a technology investment priority in the hybrid working era, and 40% intend to spend more on IT training for staff.[15] If your competitors are amongst these, you don't want to be left behind; criminals will be looking for vulnerable organisations.

Digital transformation – which has been accelerated for many organisations owing to the pandemic – will have taken care of many security and compliance issues. GDPR compliance can be automated and built into processes, for instance.

But there remain questions to ask. Where are your security vulnerabilities? Do you have the resources to find and fix them in-house, or would a third-party specialist give you peace of mind? Do all staff – from new recruits to C-suite – understand the risks inherent in hybrid working? Would training give you confidence to make critical business decisions? And do you need to launch new policies around office hardware use to mitigate the challenges caused by human behaviour?

Canon's holistic approach to information security ensures that, wherever information is accessed, managed and processed, its safeguarding is simple:

PRINT MANAGEMENT
Secure the process of sending documents to print, right up to the release of printed output at the device. Prevent data breaches by protecting print devices connected to the network and securing all user activities related to print.

CAPTURE MANAGEMENT
Secure the digitisation of paper documents and distribution to the desired destination. Improve document security by controlling access to scan functions and protecting digitised documents.

DOCUMENT & CONTENT MANAGEMENT
Secure the storing and processing of documents, whether across on-premise applications or in the cloud. Ensure compliance with data protection regulations and strengthen document and content security measures.

PROBLEMS, SOLVED: TACKLING SECURITY IN THE NEW WORLD OF WORK

Addressing human behaviour is one thing, but through smart deployment of workspace technologies, there are ways and means to reduce risks to the lowest possible level.

Canon is recognised by the IDC MarketScape as a leader in worldwide security solutions and services. Our solutions and services help to secure all documents and sensitive data – whether on paper or in digital format – across the document lifecycle, without impacting people's ability to access the information they require to do their jobs. This means that our solutions and services are secure by design, security-checked against the highest industry standards and focused on all aspects of information security.

This approach to security doesn't stop after sale. We can help to protect print and scan devices throughout their operational lifetime, from device hardening to secure disposal of devices at the end of their life, to ensure data stays protected at all times.

Regardless of where you and other staff are working, our approach ensures security right from the cloud or on-premise solution, all the way to your devices. Speaking to customers across EMEA, we have identified four common workspaces that organisations are adopting in combination to form their new hybrid working environments.

We call them the Hybrid Hubs: the Company Hub (the traditional central office), the Community Hub (co-working spaces and smaller, satellite offices), the Home Hub (remote working from home) and the Mobile Hub (working on the go – in cafes, in stations and airports or while in transit).

It's important to clearly define the different locations your workforce is using, and how they connect to one another, as each hub has its own unique security needs. Taking this workspace-specific approach means we can help you ensure information is protected from the office to the armchair.

Canon's focus on workspace evolution ensures that we consider all aspects of information security as part of the provision of every customer solution. Ultimately, digitising key business processes through a range of Canon solutions not only supports productivity and collaboration, but also gives IT teams and departments the transparency and control they need to ensure good security and compliance practices across their teams.

Information security is crucial – in a hybrid working environment more than ever – but shouldn't be scary. Take stock of your situation and take action for a successful future.

For more information, please visit: www.canon.co.uk/business/solutions

[15] https://www.computerweekly.com/news/252500569/New-normal-of-remote-hybrid-working-sees-two-thirds-of-European-businesses-increase-IT-spend

Canon Inc.
Canon.com

Canon Europe
canon-europe.com
English Edition

© Canon Europa N.V., 2022

Canon (UK) Ltd
4 Roundwood Avenue
Stockley Park
Uxbridge
Middlesex
UB11 1AF

Tel: 01895 648 000
canon.co.uk