Security in the Era of Hybrid Work

A guide and checklist for implementing comprehensive security.

The Way Businesses Operate and Information Flows Has Changed

As we evolve to new ways of working, devices, documents and data remain the life force of every business. Following the scramble to keep businesses running, flexible working has become the new normal. Have you done enough to stay protected wherever work gets done?

The data we depend on to drive business also put our organisations at considerable risk. A breach of any type can be devastating – causing chaos and distrust, plummeting stock prices and even garnering disciplinary actions and large fines from regulators.

We created this eBook to help your organisation make the best choices for protecting business documents and data by securing the print infrastructure that house them. It's designed to assist all individuals and organisations, regardless of their role or size, in comprehending the necessary procedures and policies for ensuring optimal security of their IT infrastructure. This includes external assets beyond the corporate firewall.

Refer to the checklist within this eBook often and share it with colleagues. When everyone is well-informed and on the same page, you can be more confident in your security decisions and the cyber health of your organisation.

Does your security strategy meet the demands of this new hybrid work era? Can you prove compliance beyond a shadow of a doubt? Few companies are as secure as they think.

TABLE OF CONTENTS

The Threat Is Real

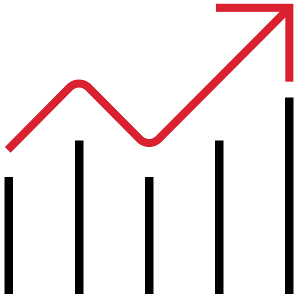
No one can afford to ignore the security of their IT infrastructure today. And the threat isn't going away tomorrow. Now more than ever, potential entry points are expanding due to the emerging flexible workplace.

Whether you have adopted flexible working practices or work with clients that have, the need for document, device and content security is more pervasive than ever before.

- Intellectual property needs to be protected from competitors
- The client's financial and personal information needs to be safe from hackers
- Employee records and personally identifiable information create concerns for Human Resources
- Industry regulations and mandates add more complexity

Larger organisations have long been targets but small and medium-sized business owners are becoming increasingly vulnerable as hackers direct more of their efforts toward them. And everyone is under pressure to meet both internal and external security policies and mandates, and prove compliance to partners, vendors and loyal clients.

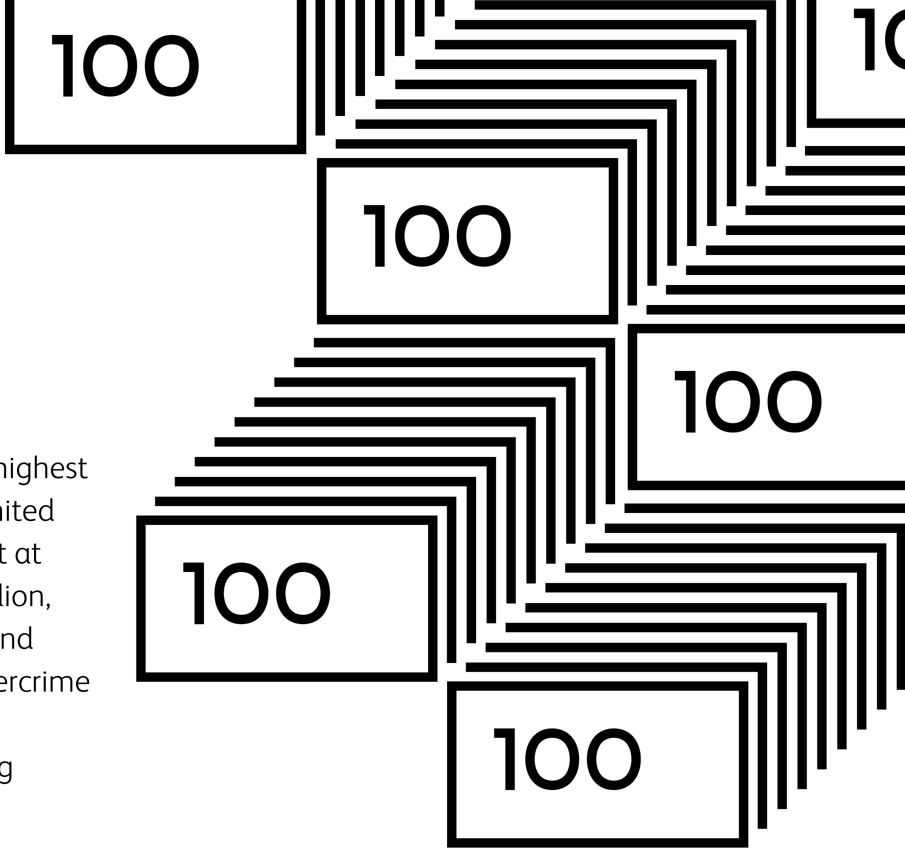
This means everyone – regardless of title, department and line of business – plays an important role and should prioritise security and compliance.



Security breaches increased for **61%** of organisations in the past year, rising to **70%** in the US and **66%** in business and professional services.

Source: Quocirca – The Print Security Landscape, 2023 (US & EU)

The Costs Are Rising



Security breaches are becoming more expensive worldwide, both in terms of financial costs and indirect consequences. These consequences include the time, effort and resources spent on notifying victims and investigating the incident, along with the negative impact on the organisation's reputation.

No company, no industry and no department is safe. Cybercriminals are launching attacks against people, households, companies, government, police departments, hospitals, schools, banks, power grids, utilities, data centres, servers, networks, PCs, laptops, tablets and smartphones.

Reaching an all-time high, the cost of a data breach averaged USD 4.35 million in 2022.

The top five countries and regions for the highest average cost of a data breach were the United States at USD 9.44 million, the Middle East at USD 7.46 million, Canada at USD 5.64 million, the United Kingdom at USD 5.05 million and Germany at USD 4.85 million.[1] Global cybercrime costs are expected to grow by 15 per cent per year over the next three years, reaching USD $10.5 trillion annually by 2025.[2]

The frequency of ransomware attacks on governments, businesses, consumers and devices will continue to rise over the next five years, reaching every two seconds by 2031.[2]

But the faster a data breach can be identified and contained, the lower the costs.

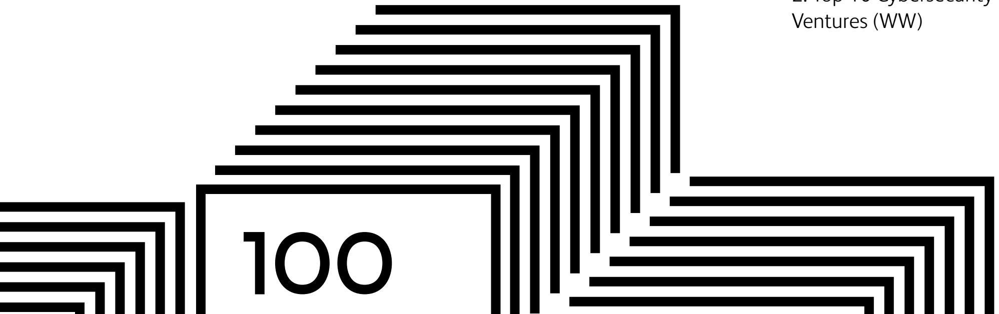
$935K

is the estimated average cost of one data breach.

Source: Quocirca – The Print Security Landscape, 2023 (US & EU)

[1] Cost of a Data Breach Report 2022 – Ponemon Institute, and sponsored, analysed and published by IBM Security® (WW)

[2] Top 10 Cybersecurity Predictions And Statistics For 2023 – Cybercrime Ventures (WW)



The Entry Points Are Numerous and Expanding

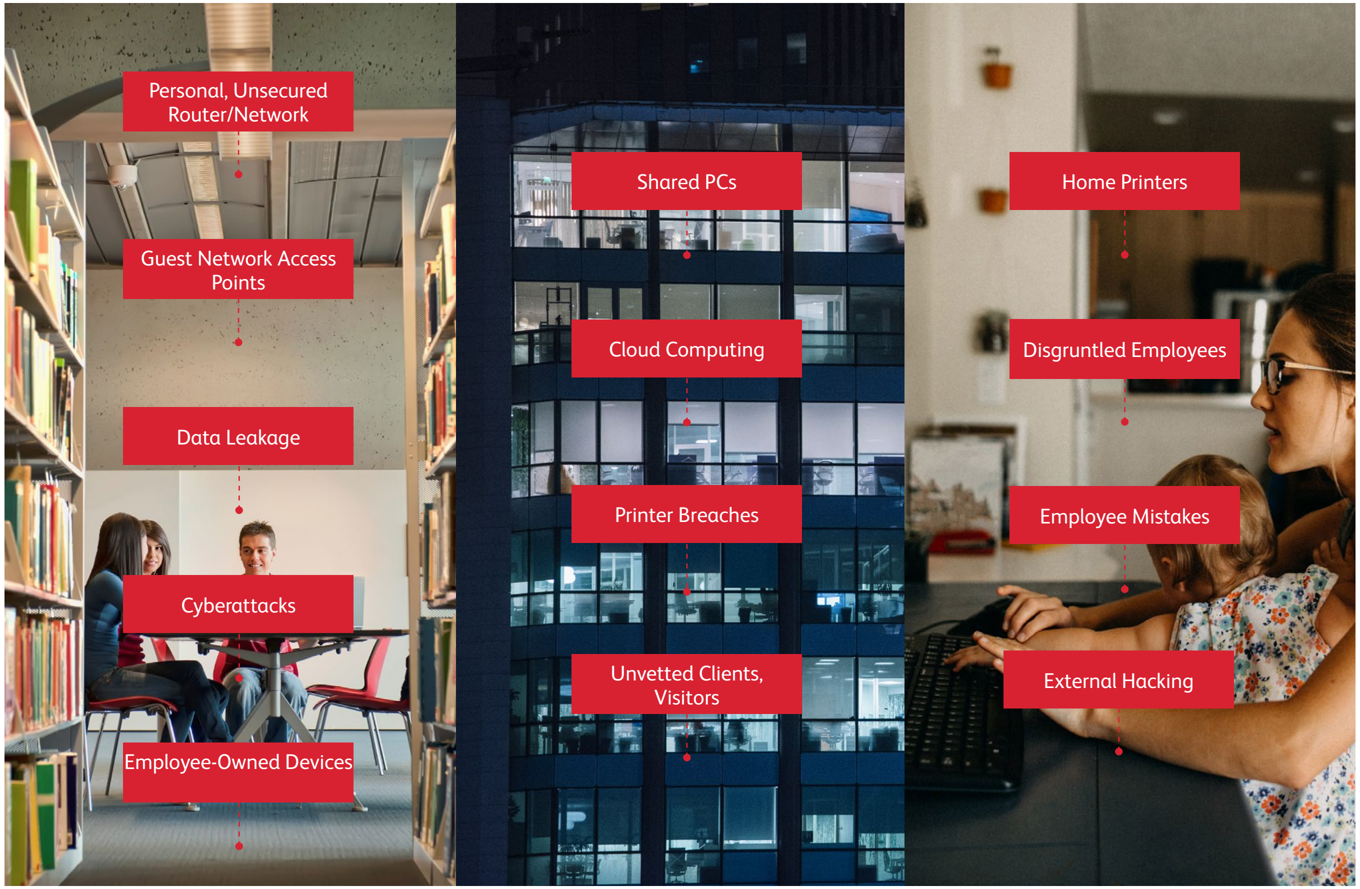
Threats arise from all aspects of your IT infrastructure and those that interact with it, both internally and externally. You now also need to consider employees or clients working from less secure homes or remote locations, even using assets not controlled by IT policies.

On average, **25%** of workforces are fully remote, **33%** are hybrid and **42%** are fully in the office.

Source: Quocirca – The Print Security Landscape, 2023 (US & EU)

Over **7%** of Windows desktop devices are running unsupported versions

Desktop Windows Version Market Share Worldwide – February 2023



Printer Breaches Happen

For hackers looking for a way into a corporate or personal network, unsecured IoT deployments like printers provide the perfect entry point. Taking a few simple steps can help mitigate the risk and stop attackers in their tracks.

WHAT TO DO? ALLOCATE OR PARTNER WITH THE APPROPRIATE RESOURCES NEEDED FOR A COMPREHENSIVE SECURITY STRATEGY AND IMPLEMENTATION.

Ensuring that your print devices are as safe as you expect them to be requires a comprehensive strategy that crosses several layers – from data and documents to people and devices and the overall rules and regulations governing your business.

Organisations, large and small, should have security policies and procedures in place for malware and attacks, data leakages and cloud computing, as well as employee policies. However, many organisations still do not have such policies and procedures for their print infrastructure.

Print-related data breaches remain prevalent, with **61%** of respondents reporting at least one data loss in the last **12** months, rising to **67%** amongst midmarket organisations.

Source: Quocirca – The Print Security Landscape, 2023 (US & EU)

The Human Factor

When security or data breaches occur, it's natural to look to IT. However, user errors or actions that fall outside of IT-recommended behaviour guidelines, cause far more problems. Your biggest cyber threats aren't malicious actors. They're your employees: They make unintentional mistakes. They use unapproved shortcuts. They strive to do more with less. As a result, they may make decisions that put your business at risk.

Click here to watch the video

WHAT TO DO?

First tap into analytics to find out how your users are working with documents and devices. Secondly, look to implement a Zero Trust Security working environment.

User analytics can answer questions like these:

- Who is printing outside business hours when few employees are working?
- A key person has resigned. What have they been printing recently?
- Has an employee scanned or emailed content to an unauthorised location like a public cloud?

Implementing Zero Trust:

- Helps reduce the human factor
- Enables authentication, so only authorised users can access what's only available to them
- Drives conscious behavioural changes

User analytics and implementing Zero Trust security can guide you to further services and solutions that drive sustainability, productivity and compliance.

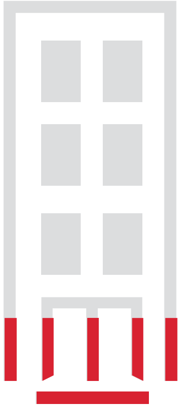
95% of cybersecurity breaches are due to human error.

Source: The Global Risks Report 2022 – World Economic Forum

Half of respondents to a recent survey said that they include print as part of their zero trust strategy, with a further 39 % planning to do so in the next 12 months.[1]

[1] Quocirca's Zero Trust Security Trends 2022 Study. (US & UK)

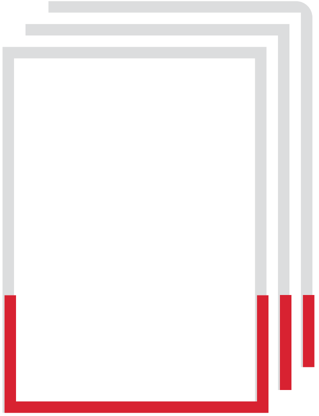
Security Measures Are Lagging



19%

of respondents are completely confident that their print infrastructure is secure.

Source: Quocirca – The Print Security Landscape, 2023 (US & EU)



On average,

27%

of IT security incidents were related to paper documents.

For

34%

of respondents, the top challenge is protecting sensitive and confidential documents from being printed.

Security concerns are growing, but security measures lag behind. Where is your organisation? Are you concerned about the security of your IT infrastructure and the documents, devices, content, and data that they hold? What could or should you be doing that you're not?

Moving Beyond Print Management

The Internet of Things (IoT) is no longer comprised of just computers and phones. Information is no longer contained in controlled, trusted environments. The cloud has changed the way businesses operate, essentially enabling access to data, applications, platforms and services anywhere, at any time.

As your workplace expands beyond the confinement of your own four walls and becomes more connected, the number of intelligent and IoT devices in your workplaces will rise, and the need to move beyond traditional Managed Print Services will rise too.

A data-driven approach to security that uses analytics to identify opportunities for cost savings and productivity is key to optimising the way employees and technology work together, leading to more productive and efficient workplaces and greater security and compliance.

HERE ARE SIX KEY THINGS TO CONSIDER WHEN CHOOSING A PARTNER TO HELP YOU CLOSE SECURITY GAPS:

1. Can they apply their solution to the right devices at the right times and create policies that are easy to enforce and comply with?
2. Do they understand your network requirements? Can they recommend solutions that are a “right fit” and utilise data to support ongoing maintenance and proactive service and support?
3. Are they focused on consistent inspection and monitoring of all devices and document processes to automatically ensure compliance across the board?
4. Can they remediate at fleet, printer and setting levels so non-compliant issues can be identified and addressed quickly?
5. Will they provide ongoing, real-time reporting to show compliance and/or highlight areas that need to be addressed?
6. Can they do this regardless of work location?

100

Companies will invest **$15 trillion** in IoT by 2025.*

*Source: vXchnge (WW)

A Comprehensive and Zero Trust Security Approach

Total endpoint protection in a mobile, cloud-driven and IoT world requires a multi-layered approach and constant vigilance, but it's not possible to monitor every endpoint manually. Despite the new challenges today brings, most security strategies don't take into account the fact that the documents, data and content that drive business today live everywhere and are available 24/7.

It is critical that your service provider takes a comprehensive, multi-layered approach to security with proactive intelligence that protects devices, documents, data and content. At the same time, compliment your Zero Trust implementation by offering solutions that seamlessly align.

68%

of organisations have experienced one or more endpoint attacks.

Source: Ponemon Institute, 2020 State of Endpoint Security Risk Study

Secure Devices
Make sure your printers have built-in protection and maximum security as soon as they are attached to the network.

Secure Fleet Management
Set security configuration policies and automatically validate compliance.

Secure Print Management
Control access to documents and provide actionable insight.

Secure Data & Content
Lock down security from unauthorised disclosure of data and content (on the device or in the cloud).

Next Steps: Identify Gaps, Gain Confidence

How confident are you that your devices, documents and data are secure, and what areas of security have you considered and implemented in doing so? It's important that you're informed about security discussions and decisions in your organisation and aware of existing gaps in order to know if you're moving in the right direction for your business.

WHAT'S NEXT?

1. Understand your company's security policies for devices, documents and data.
2. Identify and engage key stakeholders and assess your level of risk.
3. Isolate device or process vulnerabilities and weak spots, and take steps to ensure they are addressed.
4. Use the following checklist to discuss needs and gaps with your team.

Xerox® Managed Print Services is a streamlined and secure way to accelerate digital transformation and improve the way people and technology work together.

We provide interactive security monitoring and compliance from a visual and intuitive dashboard and embed printer security technologies with market-leading Trellix[3] DXL and Cisco® pxGrid platforms, enabling instantaneous, automatic threat response.

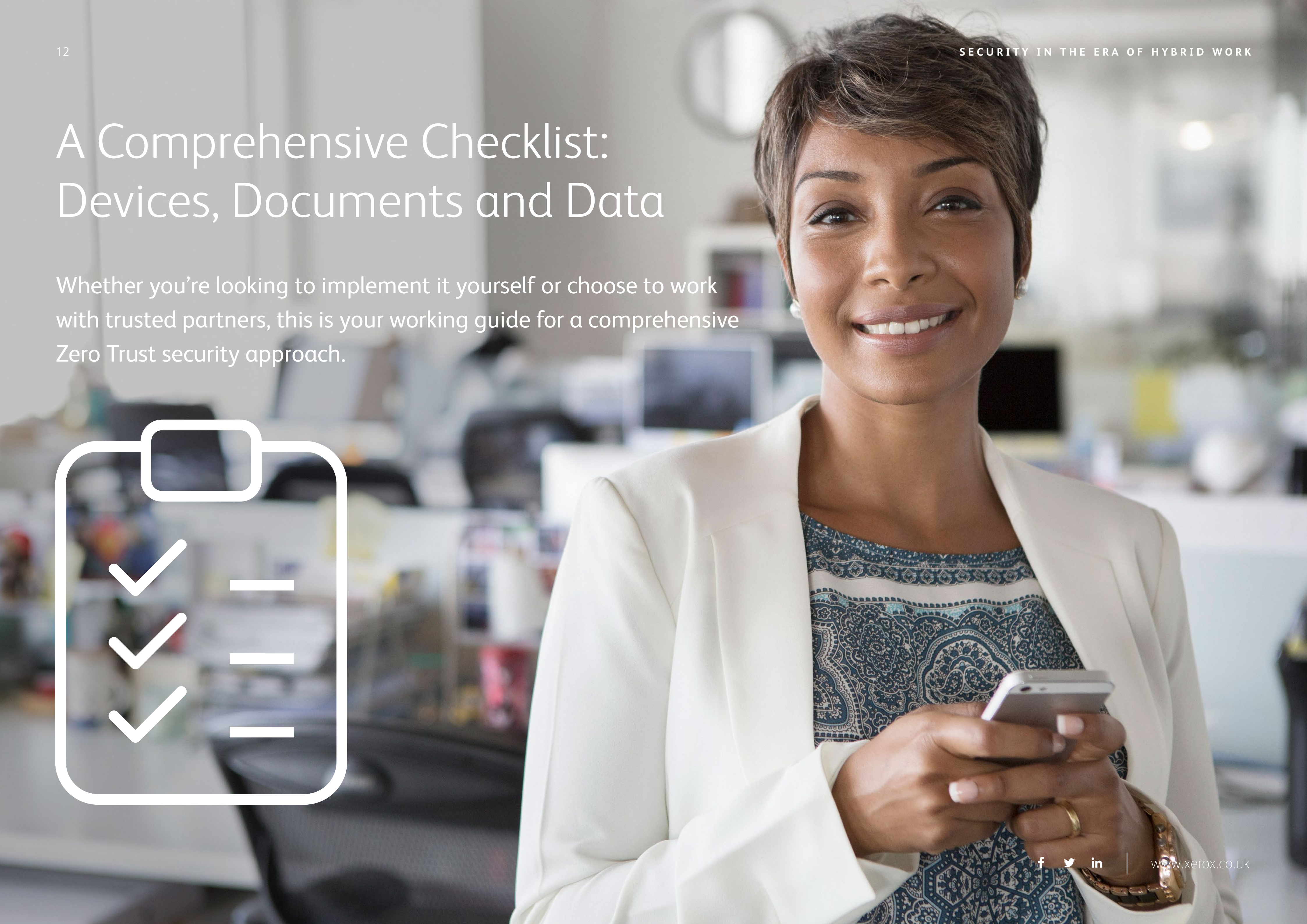
Additionally, we are the first print vendor to receive security authorisation from FedRAMP for cloud-based Managed Print Services, an element of Xerox® Managed Print Services. We are positioned as a leader in the IDC Security Marketscape as well as Quocirca Print Security Landscape reports because of our focus on security and empowering IT and end users. Together, we can create a more secure environment.

Learn more at **www.xerox.co.uk/en-gb/about/security-solutions**

[3] Trellix formerly known as McAfee® Enterprise Business.

A Comprehensive Checklist: Devices, Documents and Data

Whether you're looking to implement it yourself or choose to work with trusted partners, this is your working guide for a comprehensive Zero Trust security approach.



Security Partner Qualifications and Best Practices

Things to consider to ensure comprehensive device, document and data security.

SECURITY ANALYSIS AND REPORTING

□ Does the partner work with you to assess security needs and identify where your information lives, how it's transferred and your greatest areas of risk?

□ Does the partner provide a comprehensive security plan/strategy that encompasses devices, documents and data?

□ Does the partner help you set security policies, validate compliance, control access and lock down unauthorised disclosure of sensitive documents and data?

□ Does the partner have clear guidelines for strategies to support your Zero Trust Security initiatives?

□ Does the partner have robust technologies they can use to ensure data quality and accuracy?

□ Does the partner proactively meet with you about security and other issues?

□ Do the reports provided by the security partner bring insights into security policy implementation and at-risk devices?

RECOMMENDATIONS FOR DEVICES, PLACEMENT AND OPTIMISATION

□ Will the security partner help you select the best devices for security purposes? The most secure printers have multiple layers of security features and are capable of integrating with centralised security management programs such as Trellix[3] ePolicy Orchestrator and Cisco ISE.

□ Can the partner use analytics to thoroughly understand the devices you have today and identify areas for reduction or optimisation?

COMMITMENT TO SECURITY INNOVATION

□ Does the partner work with vendors who invest in ongoing security research, development and engineering? Xerox, for example, devotes a percentage of revenue to security and other critical research, development and engineering projects.

□ Does the security services provider utilise people, processes and technology to meet the highest standards of security compliance?

SECURITY COMPLIANCE PROGRAMME

□ Do those vendors earn accreditations, pass strict audits and receive numerous certifications for their hardware and software offerings?

MPS SECURITY SOFTWARE

□ Does the partner work with MPS vendors whose back office is certified by ISO 27001 as a secure facility?

□ Can the partner's software interrogate the multifunction printer or printer fleet for device firmware levels and determine if they align with your security policies?

□ Can security configurations be easily set and monitored, and any non-compliant devices remediated without additional manual effort?

□ Can you view confidential documents that are printed, copied or scanned that are not approved, and be notified of such behaviour?

□ Can the partner provide real-time, ongoing reporting delivered through an interactive dashboard to show compliance and/or highlight areas that need to be addressed?

□ Is sensitive data secured through user- and group-based access, password protection, content encryption, and automated retention and disposition?

[3] Trellix formerly known as McAfee® Enterprise Business.

STANDARDS-BASED TECHNOLOGY

Endpoint device security can impact your ability to comply with regulatory and industry demands.

- □ Are the products the partners deliver designed to support standards and regulations like HIPAA, Sarbanes-Oxley, the Gramm-Leach-Bliley Act, FDA 21 CFR Part 11 and GDPR?
- □ Does the partner work with vendors who seek third-party validation of device security by participating in the International Common Criteria for Information Technology and Security Evaluation programme for certification (ISO/IEC 15408)?
- □ Do those vendors submit the entire device for evaluation, not just a security kit? This matters to high-security enterprises like government agencies purchasing multifunction printers with storage drives. It ensures that extra protection is built into the device.

Support Zero Trust

NETWORK AUTHENTICATION

Security improves when administrators limit access to users based on their role/function.

- □ Are authorised users required to log in with a password or an ID card for secure access to device functions?
- □ Can these authentication and authorisation sessions be audited?
- □ Have single sign-on (SSO) and multi-factor authentication (MFA) been implemented for added security?

INFORMATION ACCESS

- □ Can confidential content use be flagged and monitored?
- □ Can notification of such unauthorised access be sent?
- □ Can you limit and track who has access to confidential information?
- □ Are controls in place to manage this information on output devices?

DEVICE SECURITY POLICY

Consider access to network assets, not just to the information.

- □ Have you created a security policy for access and printing to network assets?
- □ As data moves in and out of multifunction devices, is it secured with cutting-edge encryption?

EMPLOYEE GUIDELINES

- □ Are there measures in place to ensure employees understand and adhere to security guidelines?
- □ Is activity from employees who break these security guidelines tracked?
- □ Do you have a policy and process for approving device firmware before deployment?
- □ Is there a process to determine the credibility of software upgrades and validate digital signatures?

Important Device Security Factors

DEVICE VULNERABILITY

- □ Do devices include a network firewall to prevent unauthorised external access to your systems through a network connection?
- □ Are there possible vulnerabilities that might expose your devices to an attack?

□ Are controls in place to protect the integrity of the device firmware, such as digital signature, encryption and verification?

□ Do devices have embedded Malware Protection?

□ Do you have a consistent way to ensure devices comply with the policies for network assets?

□ Do you have a process to enforce that only expected device behaviours occur?

□ Is automated Certificate Management available?

□ Are you able to secure the communication between your devices and your network or your employee devices?

REMEDIATION ASSURANCE

□ What happens if a device falls out of compliance with the security policy? Are you alerted when this happens?

□ Are there specific steps in place to bring it back into compliance?

□ Do you have a remediation policy?

□ Do you have a way to check that the policy is in place?

□ If a network asset comes out of compliance, can you capture data for reporting?

□ Is there an audit trail?

□ Do the devices have the ability to transfer the audit log to a SIEM or audit log server?

Document-based Information Vulnerability Factors

FAX/NETWORK SEPARATION

□ Unprotected fax connections create a potential open back door into your network. Is there a complete separation between phone lines and network fax connections?

IMAGE OVERWRITE

□ Can devices be configured to automatically overwrite files stored on the storage drives?

□ Do you have a documented policy for how you purge or destroy storage drives from machines removed from service?

Security Across the Device Lifecycle

SECURITY PATCH PROGRAMME AND COMMUNICATIONS

□ Do you have a security solutions provider that offers an active security patch programme? This means they monitor for new vulnerabilities on devices, just as OS software developers track new viruses that target software.

□ Does your security solutions provider publish security bulletins when fixes to vulnerabilities in products/software are released?

□ Can you sign up for RSS feeds and receive immediate alerts when new bulletins and patches are posted?

□ Does the vendor have a Bug Bounty programme in place to help uncover potential vulnerabilities?

STORAGE DRIVE REMOVAL

□ Do you have a Managed Print Services (MPS) partner that makes recommendations on the most effective way to rid storage drives of data?

□ Does your methodology to purge/destroy storage drives from machines removed from service comply with NIST SP 800-88r1?

□ Are trade-ins and returns that will be remanufactured overwritten or reformatted?

If you don't have everything on this list ticked off, you may need a partner to help you get there. Learn more about the best-in-class, comprehensive security solutions we provide at **www.xerox.co.uk/en-gb/about/security-solutions**

To schedule a complete workplace assessment, visit **www.xerox.co.uk/en-gb/services/digital-evaluation-form**

About Xerox

In an era of hybrid work, we're not just thinking about the future; we're making it. Xerox Corporation is a technology leader focused on the intersection of digital and physical. We use automation and next-generation personalisation to redefine productivity, drive growth and make the world more secure. Every day, our innovative technologies and intelligent work solutions – Powered by Xerox® – help people communicate and work better. Discover more at **www.xerox.co.uk** and follow us on Twitter **@Xerox**.