Are your devices, documents and data safe?

Actionable advice for comprehensive endpoint security

xerox™

What is Security?

Security is defined as freedom from danger, fear or anxiety.

Therefore how secure a business is can be defined by how well it can stand up to threats that can cause the business, its customers, and information, harm.

Security is a balance of people, process and **technology**. It requires all three to be working together in order to provide a good security solution.

The Way Businesses Operate and Information Flows Has Changed

Devices, documents and data are the life force of every business. As the digital era evolves into the intelligence era, they are central to how work gets done. But the very documents, devices and content we depend on to drive business and growth also put our organizations at considerable risk. A breach of any type can be devastating — causing chaos and distrust, plummeting stock prices, even garnering disciplinary actions and large fines from regulators.

We created this eBook to help your organization make the best choices for protecting business documents, data and content and securing the multifunction printers and devices that house them. It's designed to help everyone, regardless of their role or company size, understand what procedures and policies need to be put in place to ensure your IT infrastructure is as secure as possible, and why compliance is critical.

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

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

TABLE OF CONTENTS

03 The Threat Is Real
04 The Costs Are Rising
05 The Entry Points Are Numerous
06 Printer Breaches Happen
07 The Human Factor
08 Security Measures Are Lagging
09 Moving Beyond Print Management
10 A Comprehensive and Multilayered Approach
11 Next Steps: Identify Gaps, Gain Confidence
12 A Comprehensive Checklist: Devices, Documents and Data

The Threat Is Real

No one can afford to ignore IT infrastructure today. And the threat isn't going away tomorrow.

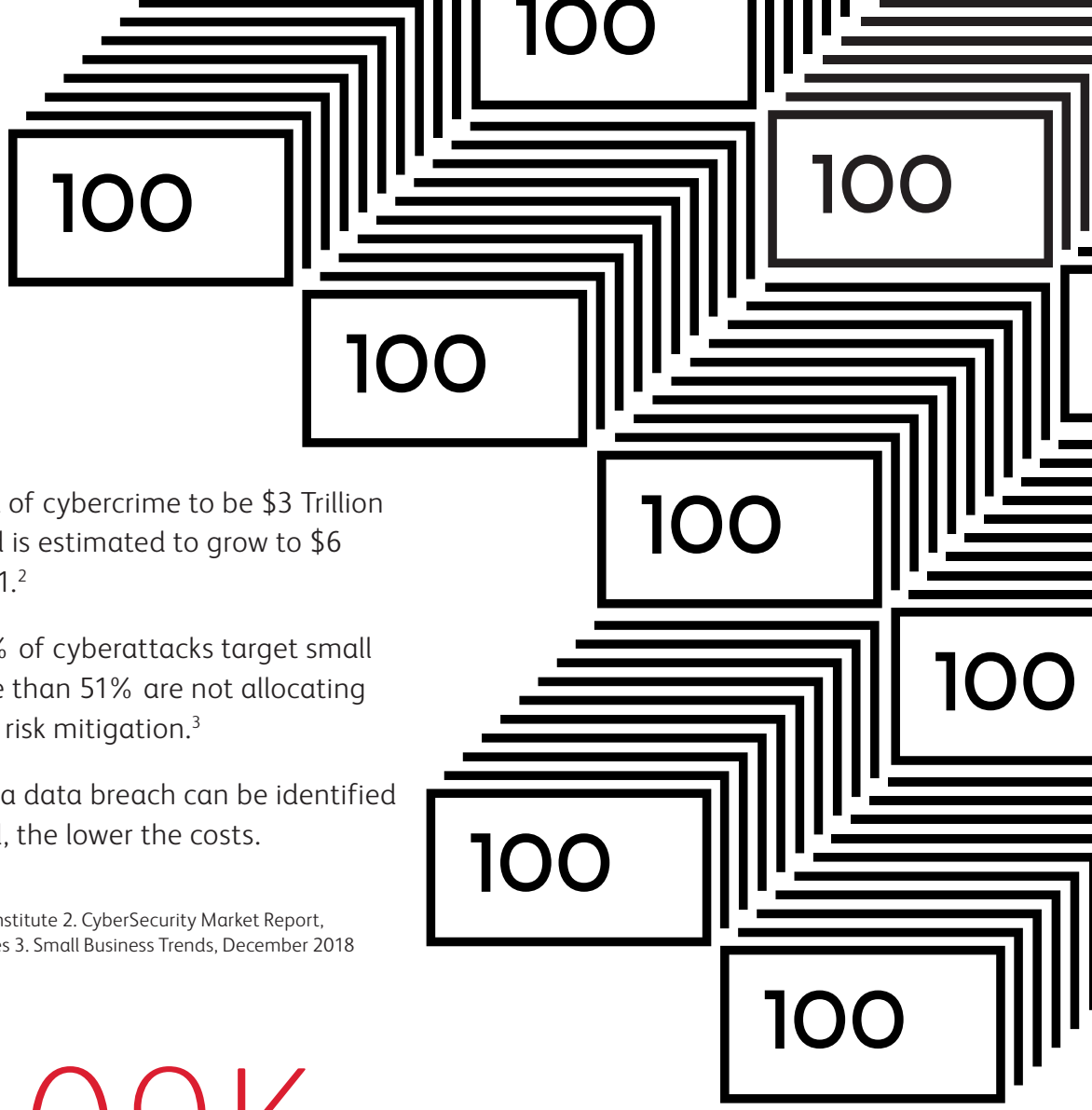
The need for document, device and content security is pervasive. Intellectual property needs to be protected from competitors. Customer financial and personal information needs to be safe from hackers. Employee records and personally identifiable information create concerns for Human Resources. Industry regulations and mandates add more complexity. Larger organizations have long been targets but small and medium size 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 customers.

Which means everyone has a role — regardless of title, department and line of business — and should be keeping security and compliance top of mind.

Protecting organizations from cyberattacks is the **#1 priority** of IT leaders in 2019.

Source: CIO Magazine

The Costs Are Rising



The global costs of a security breach are increasing, both in terms of dollars and in indirect costs such as time, effort and other organizational resources spent notifying victims and investigating the incident, as well as the loss of goodwill.

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

Cybercrime costs an organization an average of $11.7 Million.[1] The loss of customer trust has serious financial consequences. The World Economic Forum estimates the economic cost of cybercrime to be $3 Trillion worldwide and is estimated to grow to $6 Trillion by 2021.[2]

And while 43% of cyberattacks target small business, more than 51% are not allocating any budget to risk mitigation.[3]

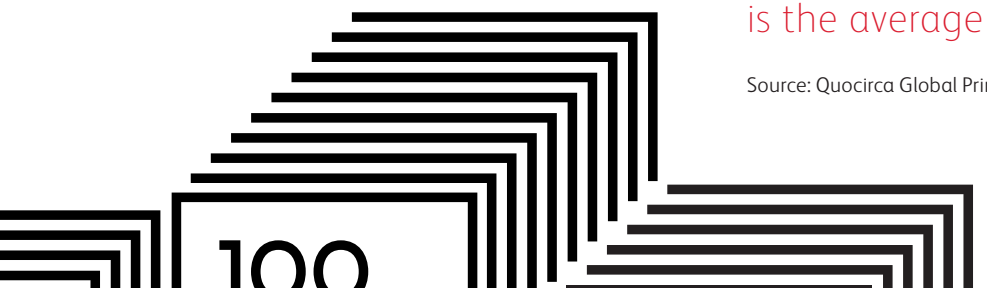
But the faster a data breach can be identified and contained, the lower the costs.

Source: 1. Ponemon Institute 2. CyberSecurity Market Report, Cybersecurity Ventures 3. Small Business Trends, December 2018

$409K

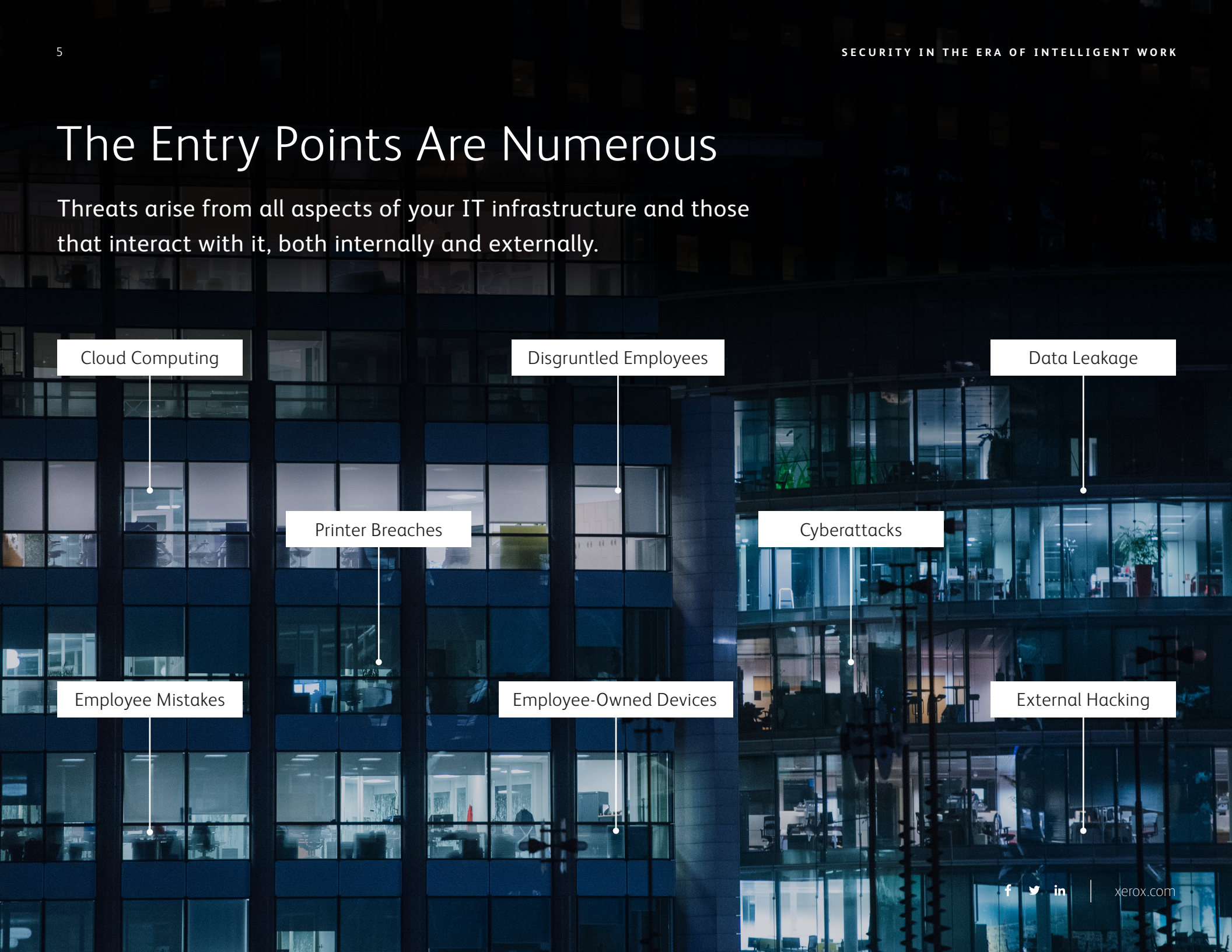
is the average cost of a print-related data loss.

Source: Quocirca Global Print Study, 2019



The Entry Points Are Numerous

Threats arise from all aspects of your IT infrastructure and those that interact with it, both internally and externally.



Printer Breaches Happen

For hackers and malware looking for a way into a corporate network, unsecured IoT deployments like printers provide the perfect entry point. And small-to-medium businesses that devote minimum funds and resources to data defense are equally vulnerable — and easier to attack.

WHAT TO DO? ALLOCATE THE APPROPRIATE FUNDS 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, to the overall rules and regulations governing your business.

Organizations 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 organizations still do not have such policies and procedures for their print infrastructure.

59%

of organizations reported a print-related data loss incident in the past year (70% for retail).

Source: Quocirca Global Print Security Study, 2019

The Human Factor

When security and data breaches occur, it's natural to look to IT. But IT security breaches are few and far between. User error or actions that fall outside of IT recommended behavior guidelines cause far more problems. Your biggest cyberthreats aren't malicious actors. They're your employees: They make mistakes. They find shortcuts. They strive to do more with less. As a result, they make decisions that put your business at risk.

WHAT TO DO? FIRST TAP INTO ANALYTICS TO FIND OUT HOW YOUR USERS ARE WORKING WITH DOCUMENTS AND DEVICES.

User analytics can answer questions like these:

- Who is printing outside business hours when few employees are working?
  Business impact: cost, security
- A key person has resigned. What has he been printing recently?
  Business impact: security
- Has an employee scanned or emailed content to an unauthorized location like a public cloud?
  Business impact: security, compliance

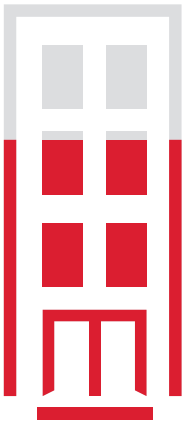
User analytics can guide you to further services and solutions that drive sustainability, productivity, security and compliance.

95%

of cybersecurity breaches are due to human error.

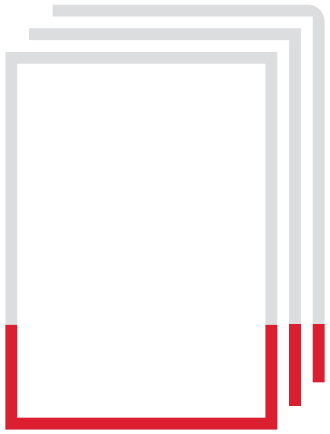
Source: Cybint Solutions

Security Measures Are Lagging



73%

of organizations are concerned about document-related security breaches.



Only

24%

are confident their document infrastructure is protected.

50%

of organizations do not have formal security policies

Source: Quocirca Global Print Security Study, 2019

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

Moving Beyond Print Management

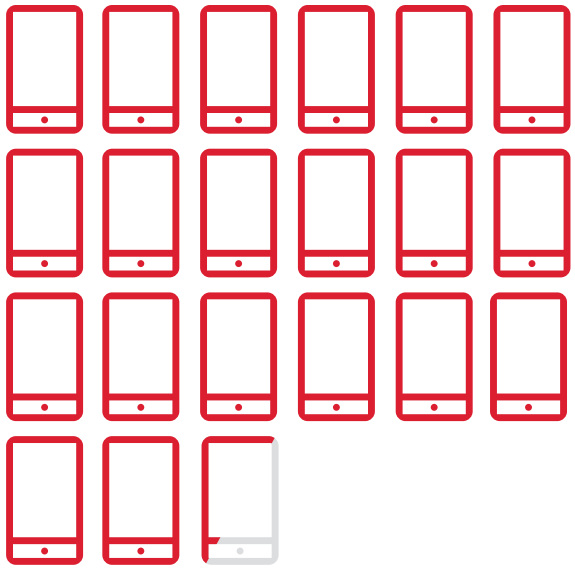
The Internet of Things (IoT) is no longer comprised of just computers and phones. Information is no longer contained in controlled, protected environments. The cloud has changed the way businesses operate, essentially enabling anywhere, anytime access to data, applications, platforms and services.

As your workplace becomes more connected and the number of intelligent and IoT devices in your workplace rises, the need to move beyond traditional Managed Print Services rises, too.

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

HERE ARE FIVE 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, and can they recommend solutions that are a "right fit" and utilize data to support on-going 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 a fleet level, a printer level and a setting level so non-compliant issues can be identified and addressed quickly?
5. Will they provide on-going, real-time reporting to show compliance and/or highlight areas that need to be addressed?



There will be 20.4 Billion IoT devices by 2020,* and companies will invest $15 Trillion in IoT by 2025.**

*Source: Gartner
**Source: vXchnge

A Comprehensive and Multilayered Approach

Total endpoint protection in a mobile, cloud-driven, IoT world requires a multilayered 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, multilayered approach to security with proactive intelligence that protects devices, documents and data and content.

Secure Devices
Make sure your printers have built-in protection and maximum security right out of the box.

Secure Device Management
Automatically validate compliance.

Secure Documents
Control access to documents and provide actionable insight.

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

70%

of security personnel believe that the threat to endpoint security has increased significantly.

Source: Ponemon Institute, 2018 State of Endpoint Security Risk study

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 organization and aware of existing gaps in order to know if you're moving in the right direction for your business.

WHATS 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® Intelligent Workplace 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 McAfee® DXL and Cisco® pxGrid platforms, enabling instantaneous, automatic threat response.

Additionally, we are the only print vendor to receive security authorization from FedRAMP for cloud-based Managed Print Services, an element of Intelligent Workplace Services, and we are positioned as a leader in the IDC Worldwide Contractual Print and Document Services Vendor Assessment because of our focus on security and empowering IT and end users.

Learn more at
www.xerox.com/SecuritySolutions

A Comprehensive Checklist: Devices, Documents and Data

Your working guide for comprehensive security.

Security Partner Qualifications and Best Practices

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

SECURITY ANALYSIS & 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 unauthorized disclosure of sensitive documents and data?
- ☐ 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 policies implementation and at-risk devices?

RECOMMENDATIONS FOR DEVICES, PLACEMENT AND OPTIMIZATION

- ☐ 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 centralized security management programs such as McAfee ePolicy Orchestrator and Cisco ISE.
- ☐ Can the partner use analytics to thoroughly understand the devices you have today and identify areas for reduction or optimization?

COMMITMENT TO SECURITY INNOVATION

- ☐ Does the partner work with vendors who invest in ongoing security research, development and engineering? Xerox, for example, has many research centers worldwide and devotes a percentage of revenue to security and other critical research, development and engineering projects.
- ☐ Does the security services provider utilize people, process and technology that meet the highest standards of security compliance? Xerox is the only Managed Print Services (MPS) provider that is certified by the US Federal Government.

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 behavior?
- ☐ 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?

About Xerox

In an era of intelligent 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 personalization 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.com** and follow us on Twitter @Xerox.

xerox™