Canon

THE 5 PILLARS OF SECURITY

Foundational Elements of Security

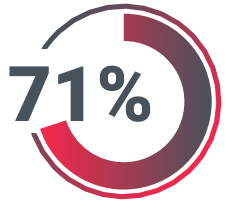
Implementing a five-layer approach to securing your critical business information

Threats—and Consequences—are More Dire than Ever

Cybersecurity continues to be a major issue facing corporations and government agencies, and Keypoint Intelligence studies consistently have shown that cybersecurity is viewed as the top priority for IT managers and decision makers surveyed. Such urgency is fueled by the successive high-profile security breaches that get covered in the media, actual experience with security breaches or attempts, and steep penalties tied to security violations for heavily regulated industries such as healthcare and financial services. In fact, the financial and reputational repercussions of one security breach could potentially force a business to close its doors.

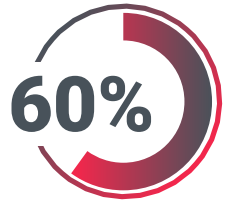
$9.36 million[1]

The average total cost of a data breach for a U.S. business, including any ransom, productivity impacts, the cost of response and remediation, and reputational damage.



An estimated 71 percent of businesses paying ransomware demands do not receive all—or in some cases, any—of their data in return.[2]

60% of small businesses go out of business within six months of a cyberattack.[3]



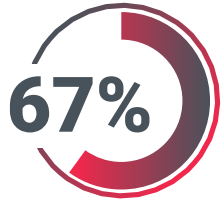
There is no way to eliminate 100 percent of the security threats coming at an organization. Moreover, mitigating issues are not a "one and done" proposition. The key to a successfully cybersecurity strategy is a layered approach that helps to address five core elements: Cybersecurity, Device Security, Print Security, Document Security, and Information Security.

[1] 2024 IBM Cost of a Data Breach Study
[2] Coveware 2023 Ransomware Recovery Report
[3] The National Cyber Security Alliance (NCSA)

Cybersecurity

Unfortunately, cyber threats are on an upward trajectory and show no signs of slowing. The ready availability of hacking tools on the Dark Web—many made more potent by artificial intelligence (AI)—has put means of attack into more unscrupulous hands than ever before. For example, AI-powered code generators can be used to create malicious programs (such as malware and exploit kits) more quickly and efficiently than a human could, leaving the hacker more time to widely deploy the malware. Hence, "security through obscurity" (whereby an organization assumes they are not a big or well-known enough target) is also no longer a viable defense. Today's automated tools troll the Internet for any open targets, regardless of company size or industry.

The biggest threat to any organization—employees falling prey to social engineering spoofs such as phishing scams—is also complicated by AI. The new WormGPT service, a dark AI tool modeled after the popular ChatGPT generative-AI content creation tool, will spit out carefully crafted, legitimate-sounding phishing emails with none of the tell-tale poor grammar and odd phrasing typically found in human-generated spoofs. This makes ongoing Security Awareness Training (SAT) for employees even more important, to help ensure that workers across the organization can recognize social engineering scams (which may arrive via email, phone calls, text messages, or social media services) and react according to the company's policy.



67 percent of breaches involved external actors, predominantly organized crime syndicates (75 percent).[5]

24 percent of breaches were caused by a human element, such as use of misused/stolen credentials or falling prey to social engineering attacks.

Of course, SAT is just one element in good cybersecurity hygiene. The National Institute of Standards and Technology (NIST) has devised an updated version of its well-known cybersecurity model for organizations to follow to ensure best practices when it comes to thwarting attacks. The Framework for Improving Critical Infrastructure Cybersecurity (known as the Cybersecurity Framework, or CSF, for short) can be used for the implementation of an organization-wide cybersecurity strategy and helps ensure consistency of procedures across departments. Moreover, it serves as a touchstone should an attack occur, so personnel have a roadmap for a coordinated response.

[4]Verizon 2023 Data Breach Investigations Report (DBIR)
[5]Source Verizon 2024 DBIR.

NIST Cybersecurity Framework

IDENTIFY
Develop an understanding of the cybersecurity risks to systems, people, assets, data, and capabilities that exist.

RECOVER
Identify appropriate activities to restore any capabilities or services that were impaired due to a cybersecurity incident. Then implement any required improvements to systems and processes based on lessons learned from the incident.

PROTECT
Outline appropriate safeguards to help keep IT systems and company information safe, without interfering with critical business functions and taking into account the organization's risk tolerance.

RESPOND
Since a fast and appropriate response will make all the difference, organizations need to have a response plan in place before an event occurs.

DETECT
Implement products and technologies to help identify cybersecurity events in real-time to ensure timely discovery and alerting of any suspected cybersecurity breaches.

GOVERN
Encourage stakeholders within an organization to make and execute internal decisions to support the organization's cybersecurity strategy, and recognize that cybersecurity is a major source of enterprise risk—ranking alongside legal, financial, and other risks as considerations for senior leadership.

Device Security

When it comes to endpoint cybersecurity, the focus of IT departments tends to be on securing traditional targets such as network infrastructure, PCs, and servers. However, relatively little attention is paid to printers and multifunction devices (MFDs) that are every bit as vulnerable. After all, today's business-class MFDs sit at the intersection of the network and the Internet (a nexus desired by cybercriminals) and have a full operating system embedded in firmware to allow sophisticated processes to run natively on the device—which means they have the power needed to run even sophisticated malware.

To lessen the likelihood of a print device being used as a conduit for a breach, leading manufacturers have hardened the security of business-class MFDs. These security features include:

- ✓ **Strong multi-factor authentication schemas** to ensure only authorized users are accessing the device and the network it is attached to.
- ✓ **Authorization control** to set access and usage restrictions.
- ✓ **Encryption** for device communication, along with using only secure ports and protocols.
- ✓ **Trusted Platform Module (TPM) security** to ensure data written to the device's drive is encrypted and digitally signed.
- ✓ **Hard-drive overwrite** to keep device-resident data safe.
- ✓ **Proprietary operating systems** that are not widely distributed, which makes coding malware to run on the device a challenge.
- ✓ **Built in whitelisting capabilities** that ensure that only known, approved apps with digitally signed certificates will run.
- ✓ **Periodic BIOS and/or firmware integrity checking** to see if there have been any unauthorized changes, which could indicate a breach.
- ✓ **Integration with SIEM (security information and event management) solutions**, which collect and analyze machine data from across an organization's IT environment to provide real-time indicators of potential security incursions.
- ✓ **Advanced fleet-monitoring utilities** that allow IT administrators to create templates for desired security settings for devices, apply those settings, monitor devices for changes to those settings, and automatically remediate settings that get changed from what is desired.

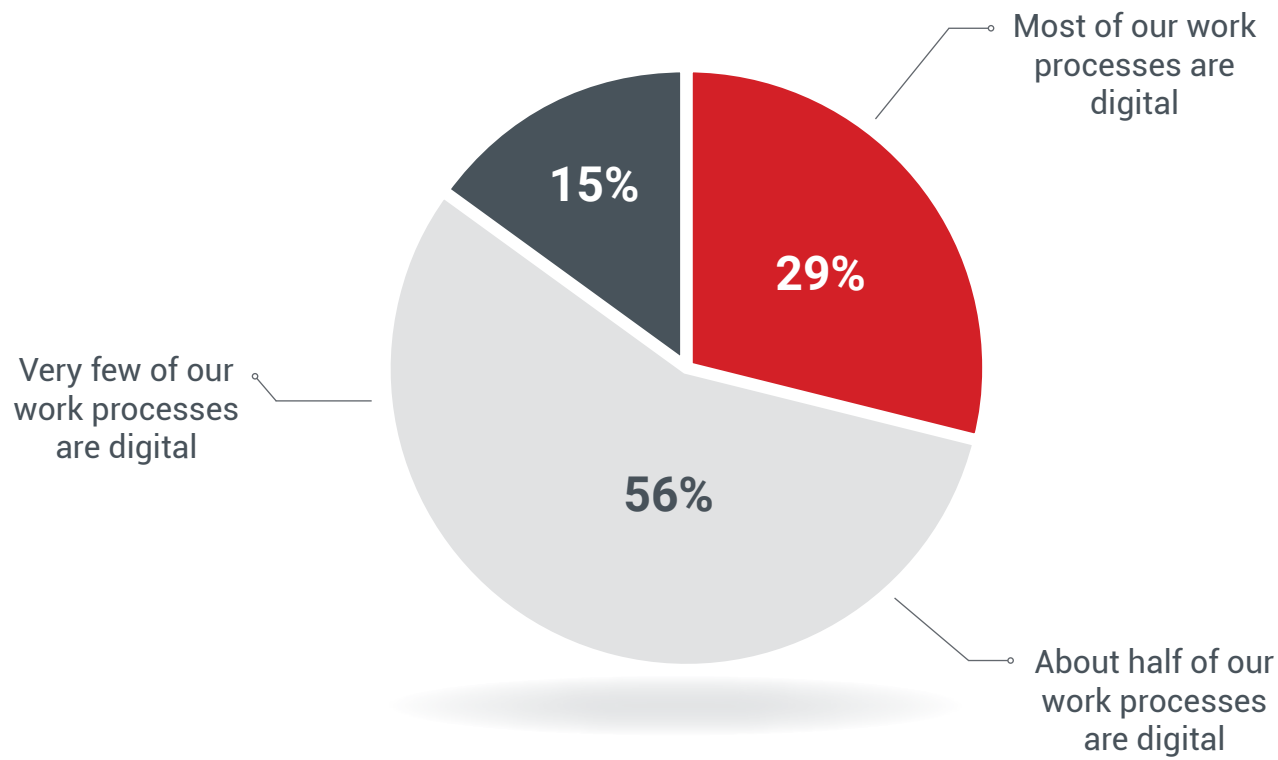
Print Security

Hardcopy output can also pose a security and privacy risk, since printed material can contain a significant amount of confidential or private information. These types of breaches can be as damaging as when electronic files are stolen, especially in environments such as Healthcare, Education, and Financial Services, where sensitive information is exchanged daily.

So, in addition to the device security measure outlined here, organizations should add an extra layer of a robust output management solution. Such a server- or cloud-based system can help ensure that documents sent to the MFD are held back until the authorized users authenticates while physically at the device to safeguard that sensitive documents are not left on the output tray for others to see. These solutions can also provide an audit trail, so the IT department can recreate who printed what and when.

Document Security

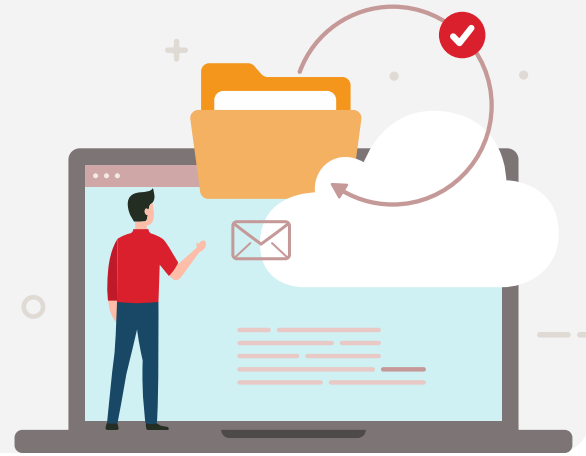
Thanks to organizations' ongoing digital transformation (DX) initiatives, an ever-increasing volume of information is stored in digital form. In fact, in a recent Keypoint Intelligence research study of 300 U.S.-based IT decision makers, 85 percent of respondents indicated that half or more of their organizations' document-centric workflow processes are now digital.



Source: Keypoint Intelligence 2023 IT Decision-maker Survey (US)

Storing electronic documents in a secure content management system is a must. In addition to the convenience of searchability, efficient workflows, and anytime/anywhere access, a well-designed system should deliver these security benefits:

- ✓ **Encryption** for stored documents.
- ✓ **Authentication** to ensure that only authorized users have access to the documents assigned to them or their department.
- ✓ **Audit trails** so managers can see who created, edited, printed, and forwarded documents.
- ✓ **Version controls** in order to "roll back" documents to an earlier version, if needed.
- ✓ **Retention policies** to help organizations in heavily regulated industries remain compliant.



Information Security

Keeping documents (and the data they contain) secure when they are in your possession is one thing. However, securing those documents when they must be sent out to partners, customers, and collaborators is a different story. An information security solution can help ensure that documents sent out-of-house can be viewed only by the intended recipient(s). Moreover, such a solution will let you set an "expiration date" on that shared document (after which it cannot be accessed) as well as set controls for actions allowed on a protected document, such as limiting editing, printing, and forwarding.

Choose a Trusted Partner

Organizations shouldn't take on all of these challenges on their own. Doing so would severely tax already-overburdened IT departments, not to mention there are simply not enough security experts to go around.

There were an estimated **638,000** unfilled cybersecurity jobs in the U.S. in 2022, and that number is expected to grow to **735,000** by 2025.

Indeed, Keypoint Intelligence' research has also shown that selecting the right partner is critical, and that approximately 50 perecent of IT buyers plan on outsourcing some aspects of their security needs to a trusted partner. Reasons include lack of IT bandwidth in-house, lower cost compared to full-time IT staffing, and the desire for specialized IT security expertise.

Why Canon U.S.A.?

Establishing and maintaining a security posture that adequately balances risk and business productivity is top of mind for many business leaders. Canon U.S.A.'s mission is to offer our customers solutions and services that can enable business growth, provide improvements in productivity and efficiency, and protect information as it flows both inside and outside an organization.

Canon U.S.A.'s Five Pillars of Security presents a portfolio of cybersecurity products and services in a comprehensive way that groups solutions in functional areas. Cybersecurity is a key component of our Five Pillar approach.

Produced by: KEYPOINT INTELLIGENCE

Canon

1-844-50-CANON | usa.canon.com/security

This analysis was commissioned by Canon U.S.A., Inc.

03.11.25/25-0134-9170