Cybersecurity: 4 Overlooked Areas (and How to Secure Them)

THE 5 PILLARS OF SECURITY

Most organizations are up to speed when it comes to cyber-threats to their network and computing devices. They have tools in place - firewalls, anti-malware software, and so on to thwart attackers. But developing an effective security posture for the modern workplace necessitates a defense in depth approach with many layers of protection involving a combination of people, processes, and technology. Here are some potential vulnerabilities that often get overlooked.

1. Print Devices

There's no shortage of attention paid to servers and PCs when it comes to cybersecurity. What about other classes of endpoints, such as printers and MFPs? With their robust operating systems and key placement at the intersection of the Internet and the corporate network, printers and MFPs are an ideal target for cybercriminals looking to gain access to the network or to enlist "bots" to serve in a DDoS attack. The threat is not just theoretical: high-profile breaches have occurred (or have been attempted) that involved a networked MFP as the nexus.

Some OEM's have developed their products to work in Zero Trust architectures and have features and functionality that align to the NIST Cybersecurity Framework. Look for tight integration between the device and leading Security Information and Event Management (SIEM) platforms, so any suspicious events can be reported and flagged for attention in real time.

2. Stored Documents

Documents (and the information they contain) are the targets of most hacks, since they can contain sensitive—and hence valuable—corporate, employee, and customer information. And even if the hacker doesn't want that information per se, locking it up and keeping you from it via a ransomware attack can lead to significant expense for your organization and perhaps negative PR that can damage your organizations reputation.

A centralized, well-managed document management platform can help protect your documents and the data they contain. Classification and governance are two key controls of a well-managed document management system. These systems also offer other valuable controls such as version control, retention policy management, and auditing capabilities—in a tamper-proof environment.

Each document or record involved in a data breach costs a company an average of

$165

per record when all costs are factored in—*an all-time high.*[1]

3. Distributed Documents

An information management system lets you protect documents when they are at rest and in your possession, but business processes often require documents to be distributed to clients and customers. An enterprise digital rights management (eDRM) system allows you control over documents as they circulate more widely. With an eDRM solution, you can specify who can open a document, who can edit it, whether it can be forwarded or printed, and more. This helps ensure that the document is only seen by its intended recipients, even if it is intercepted along the way or inadvertently makes its way into the wrong hands. You can even set expiration dates so the document "self-destructs" after a specified time.

4. Paper Mail

The Digital Transformation (DX) revolution we have seen over the past few years has moved more and more documents to digitized form. In fact, in Keypoint Intelligence's 2023 IT Decision-maker Survey, 80% of US respondents indicated that a "paperless office" was an achievable goal for their organizations within five years. Of course, you can't control where clients, suppliers, and customers are along their DX journeys, so inevitably some documents will arrive on paper via snail mail. In the current business climate of hybrid working environments, postal mail is no longer an effective modality—it can also be a security risk and prevent timely delivery to remote workers. A digital mailroom solution is an answer. Incoming mail is scanned and delivered electronically according to a company's desired workflow (for example, via email or to an information management system) so the intended recipient winds up with it. This system can be a pivotal positive contributor to the total experience (TX) of the organization and its clients.

---

[1] IBM Security 2023 Cost of a Data Breach Report

THE 5 PILLARS OF SECURITY

- DEVICE SECURITY
- DOCUMENT SECURITY
- PRINT SECURITY
- CYBERSECURITY
- INFORMATION SECURITY

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 usa.canon.com/security