Partners in Data Protection

You don't have to be a big corporation to care about data security. Most companies have Intellectual property, strategic plans, or personal data to protect. And while growth in cloud-hosted software and services, remotely accessible wireless devices, and the Internet of Things, bring efficiency and unprecedented opportunity to share and collect data, they also make businesses more vulnerable.

Businesses today face threats from unauthorized access to or disclosure of information, cyber theft and ransom ware, and vandals that aim to shut down websites or networks through denial of service. These data thieves and miscreants seek vulnerabilities, the places where networks can be breached most easily, where information in documents or hard drives can easily be obtained.

Because security threats never cease, data security cannot be accomplished through "one-and-done" solutions. Blending innovative technology with expertise in work processes, we partner with our customers to prevent data from getting into the wrong hands inside and outside the work environment. We take a strategic approach to printer security that includes intrusion prevention, device detection, document and data protection, and external partnerships with our information security vendors. Our enterprise content management (ECM) systems run on servers that incorporate the latest security features for cloud-based server technology.

With Xerox, what's more secure is also more efficient

Security measures are sometimes viewed as necessary nuisances – think TSA lines at the airport. But at Xerox, we've found manage print services can strengthen security while streamlining work processes and saving resources. Take the badge-to-print feature on our multifunction printers. Documents left at the printer pose data security risks, but with badge-to-print, employees simply scan their badge at the printer to collect outputs, ensuring document security management while saving

paper. At the same time, Xerox user analytics features help identify compliance breaches and monitor equipment use.

Counterfeit documents also threaten legitimate companies across the globe. Adding fraud deterrent technology such as Xerox® Specialty Imaging to event tickets, ID badges, transcripts, coupons or other valuable documents can reduce the risk of unauthorized duplication.

Protecting all points of access

Hackers look to breach corporate networks for "street cred," while nation states may search for trade secrets or product specifications. Printers often provide the easiest point of entry, especially if default passwords, which often can be found on the Internet, have not been changed. Once in the network, a patient hacker can methodically collect information, such as email formulations, with which to conduct phishing scams. Hackers may also gain access to servers and install malware that compromises network security. In response, we offer systems like the AltaLink family of high-volume printers that are username and password protected. These systems provide our customers with McAfee whitelisting technology, which constantly monitors for malicious malware and automatically prevents it from running. We also provide our business partners with printer security best practices.

Layers of defense

Networks can be compromised in multiple ways from a number of different places. That's why we take a multilayered approach to data security. Through compliance programs, we ensure the reliability and security of our suppliers. We anticipate potential security threats and design products with features that support efficient and secure workflow. We supply our customers with timely security bulletins to ensure an ongoing partnership well beyond their purchase.

*Document Security and Compliance: Enterprise Challenges and Opportunities, InfoTrends, April 2013.