Securing the Office of the Future

BY HIRO IMAMURA, CANON U.S.A

ORGANIZATIONS AND individuals today have access to an excess of data and information, a direct result of the evolving and emerging technologies entering the workforce. While companies have been able to reap the benefits of this data to optimize processes, better reach consumers, and become more efficient overall, they must also now navigate new ethical and legal land mines to ensure that they are sharing and using data responsibly. Recent events and regulations are resurfacing this issue as a global priority and, as a result, enterprises and workers are rightfully paying more attention to information security.

Especially in the office of the future, new technologies such as artificial intelligence, machine learning, robotics, and the cloud – just to name a few – are increasingly merging with the workplace, impacting jobs and trafficking greater volumes of data than ever before.

Specifically focusing on security, there is a lot to consider. Business leaders and decision makers must, in a way, double as IT professionals as they take on the challenge of attempting to integrate these next-generation technologies into the workplace in order to stay on the cusp of change and increase productivity and efficiency, without simultaneously compromising on security.

It is a challenge that business leaders understand they must tackle in the immediate future. According to a December 2017 study of 500 CIOs and IT decision-makers,* 84 percent of business leaders say that network security is critical to digital transformation in the workplace.

The evolution of network security is not limited to only new and emerging technologies. Even legacy hardware and older technologies could prove to be security vulnerabilities as the enterprise network opens itself to new solutions inside and outside of the office. With technology allowing for greater flexibility and connectivity for workers all of over the world, we can no longer just be concerned about the technology that is inside the four walls of the office.

As employees share more data and content digitally, and the sharing economy continues to exert its influence on the office of the future, IT and data security leaders will have to invest heavily in network and device security solutions to allow workers the freedom to work and collaborate remotely and with access controls. They should also prioritize security solutions that protect information as it travels both within the network and into the cloud.

Notably, however, it seems some enterprises may be overlooking print and software solutions in their digital transformation strategies. While to those in this industry, it may seem obvious that print and software solutions are the heart of any office, and therefore should be top of the priority list when considering new network and device security protocols, the same IDC study found that only 37 percent of business decision-makers surveyed see significant security risk in employees printing, scanning, faxing or copying documents. This is surprising given how often it seems employees accidentally (or intentionally) distribute private data using shared office solutions in highly publicized information leaks, which leads to potential fines, reputation damage, or other negative scrutiny for a business. Organizations should take the time to consider how to improve print and software solutions to help secure their network and comply with the expectations of today's workforce.

Print solutions

Companies should invest in print solutions with advanced security capabilities, such as authentication solutions, secure release printing and usage monitoring systems to monitor behavior. These tools can help restrict access to specific roles or individuals, and some solutions even come equipped with software that can send email alerts when specific keywords that have been identified are printed, scanned, faxed or copied. Other considerations include device hardening and highly secure document and mobile printing — for example, including the creation of encrypted PDFs with a password to unlock when users scan documents at a compatible MFP.

Another useful feature is the availability of a common source code across all MFP models in a line, making it easier to update products with additional features to address newly discovered security vulnerabilities with regular firmware updates across the product line. This is particularly important in an ever-evolving security climate to build security software that can not only address existing threats, but evolve in tandem to handle new, previously unidentified problems.

Software

To complement a strong MFP fleet and a secure technology portfolio in a business, security software is essential. Cloud connectivity and other security features can help improve the control and efficiency of MFPs. Security solutions are available that deliver detailed oversight of an organization's document-related activities on compatible devices. Look for permission settings that are easily configurable and highly customizable, ensuring that only authorized persons are given access to view and/or modify specific documents.

In the age of remote working trends, it is important to provide solutions that allow employees to access paper in the office, on smartphones, or tablets to capture data whenever – and wherever – they need it in today's digital era. Cloud-based apps and solutions can address many of the headaches and vulnerabilities that come with sending and receiving large files, including sending confidential information in the form of bulky, unprotected attachments. Software that allows the separation of attachments from emails to cloud-based platforms can be particularly helpful for businesses tasked with maintaining sensitive files for audit, including those in legal, finance and healthcare.

Putting it all together

Notorious, large-scale attacks impacting major corporations have made most companies aware of the importance of security; however, many underestimate the importance of device protection when assessing necessary security investments and how it fits together with network and software protection for a comprehensive security suite for the office. With more opportunities for employees to connect from anywhere, and shared office equipment or BYOD (Bring Your Own Device) policies becoming the norm, enterprise vulnerability to attacks from outside forces or careless employees is increasing.

When leaders and decision makers look to optimize their workplace for the future, all hardware, software, and network systems should be considered for an upgrade in order to create an aggressive and holistically secure portfolio. While access to data and information has created heightened risks, it's also created an opportunity for enterprises to refresh their technology portfolio to not only protect confidential information across the organization, but also increase productivity and efficiency in the office of the future.

* *IDC InfoBrief, sponsored by Canon, Digital Transformation & Emerging Technologies: The Canon Office of the Future Survey, Conducted by IDC, December 2017*

contributor

Hiro Imamura
Canon U.S.A.
usa.canon.com