Client: **Confidential**

Project: **“We’re underestimating the dangers unsecured printers pose to networks” article**

portfolio

While the Internet of Things (IoT) can offer many advantages, having more “things” connected to the company network also brings increased danger.

In a recent XXXX survey of over 300 IT decision-makers worldwide, nearly 75% of respondents said their organizations experienced an external IT security threat or breach in the past year.

These attacks came from the usual suspects:

- Malware
- Viruses
- Phishing

To defend against these attacks, IT teams are also focusing on the usual suspects: Desktops, laptops and mobile devices. But they’re missing a key entry point, according to the XXX survey; just 16% of respondents considered their printer to be a high security risk. This despite a 2016 survey from research firm Quocirca that showed 63% of businesses experienced print-related data breaches.

This perception among IT professionals is affecting how they set up network security.

Why printers are vulnerable

Printers have three primary components that can be attacked:

- The OS driver
- The management tools
- The printer’s software

Organizations use printers ranging from offset and digital to multifunctional and 3D. And often, these printers installed on company networks have no default security. When it comes to deployed security protections and security controls, printers consistently trail other endpoints. The XXX survey shows only 57% of

organizations have security practices in place for printers, and only 28% deploy security certificates for printers.

Neglecting printers, though, can have dire consequences for organizations of all sizes.

Why we should care

Printers, like other networked IoT devices, can pose an alarming cybersecurity risk. Printer attacks usually focus on the information flowing through the device, but multifunction printers (MFPs) and larger network printers offer a lot of attractive morsels for hackers.

Because most MFPs can store printed data electronically, neglecting to employ strict security measures can lead to a vast array of threats:

- Print jobs stored to the printer's cache could allow hackers to gain access to sensitive personal or business information, including Social Security numbers, financial information, or internal memos and documents.
- Cybercriminals can spy on your networked devices—compromising the security of your whole network by creating an access route to any connected devices.
- Printer exploitation or vulnerability has resulted in an increase of corporate espionage and gathering of highly sensitive information.

Rethink printer risks

Clearly, printers need to be given the same priority as any other endpoint. Rethinking the risks to your printer and prioritizing this intrusion point could mean reinforcing the security of your whole network.

Want to learn more about trends in printer security and how these trends affect businesses? Check out the new white paper.