Client: **Confidential**

Project: **"Unlocked doors: Trends show printers are being left vulnerable to cyber attacks" white paper (excerpt)**

portfolio

In March 2016, thousands of printers at college campuses from Princeton to the University of California at Berkeley spontaneously shot out pages filled with swastikas and anti-Semitic messages. Some people outside of college campuses also reported hate mail mysteriously showing up on their printer tray.

The culprit behind the printings was notorious cyber hacker Andrew Auernheimer, a "hacktivist" standing for free speech and "fighting white genocide." Auernheimer told the New York Times he had sent the fliers to every publicly accessible printer in North America.[1]

Those printers make easy targets: Many publicly accessible printers—or printers that will accept print jobs from any machine on the internet—have no restrictions and aren't securely locked down. As Slate notes, printing is a sufficiently miserable process without trying to impose extra restrictions on when a printer will and won't work in the name of security.[2]

But the threat extends beyond publicly available printers and into your office. Enterprise-class printers have evolved into powerful, networked devices with the same vulnerabilities as anything else on your network.

And those unsecured entry points offer the very real possibility of cyber attacks that go well beyond anti-Semitic messages; they can offer access to your financial and private data, leading to very real business consequences.

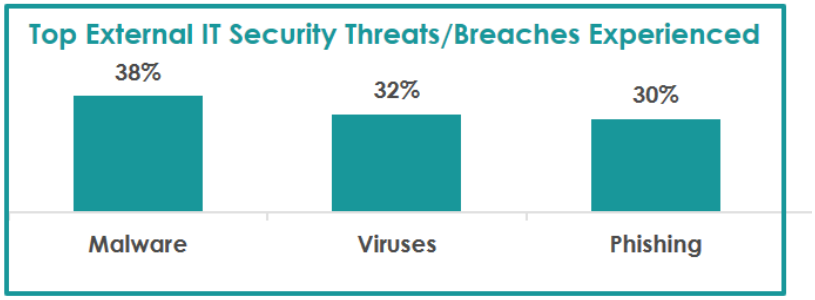
A November XXX survey of enterprise IT decision-makers, though, shows that just 16% of respondents think printers are high risk for a security threat/breach, significantly less than desktops/laptops and mobile devices.[3] That perception has tainted how IT staffs are approaching network security—while nearly three in five organizations have security practices in place for printers, that percentage is well below other endpoints—and leaving them vulnerable when there are easy solutions to safeguard that entry point.

This white paper explores trends in printer security based on the XXX survey of 309 IT decision-makers in North America, Europe, the Middle East, Africa, and

Asia Pacific, the impact of security breaches, and some of the modern build-in printer security features designed to protect against cyber attacks.

The doorways for attacks

In the XXX survey, 74% of respondents said their organization has experienced at least some type of external IT security threat or breach in the past year. Seventy percent experienced an internal IT security threat or breach, most commonly from user error, the use of personal devices for work purposes, or employees using a home or public network for work purposes.[3]



Those threats snuck in primarily through desktops and laptops, with some coming through mobile devices and a small percentage—just 16%—through printers, respondents said.[3] However, it's possible that the number of attacks striking through the printer is underestimated because printers are not being as closely monitored as PCs and mobile devices.

In another survey from research firm Quocirca earlier this year, 63% of businesses admitted to experiencing one or more print-related data breaches.[4]

We're ignoring our printers

Whatever the case, printer security is often an afterthought, the XXX survey makes clear.

Organizations are acutely aware of the importance of network, endpoint, and information security. More than a three-fourths of respondents in the XXX survey use either network security, access control/management, data protection, or device security—or a combination of those.[3]

But those solutions are deployed far less often on printers. While 83% of respondents use network security on desktops/laptops and 55% on mobile devices, just 41% use it on printers.[3]

The disparity is even wider for device security: 77% for PCs, 61% for mobile devices, and just 28% for printers. Also, only 28% of respondents said their organization deploys security certificates for printers, as opposed to 79% for PCs and 54% for mobile devices.[3]

Among protections used on general endpoint devices, the most-used security measures for printers were document security, network security, and access control, but less than half of respondents said their organization use any of those on their printers.[3]

Some companies do have printer-specific security practices, but even there, the practices are widely disparate, with no one approach being used by the majority of organizations in the XXX survey. Just over 40% of organizations deployed user authentication, and nearly 40% used administrator passwords for web configuration interface.[3]

Clearly, organizations aren't taking printer security serious enough, but they certainly should.

"Many printers still have default passwords, or no passwords at all, or ten are using the same password," Michael Howard, HP's chief security advisor, told Computerworld in June. "A printer without password protection is a goldmine for a hacker. One of the breaches we often see is a man-in-the-middle attack, where they take over a printer and divert [incoming documents] to a laptop before they are printed. They can see everything the CEO is printing."[5]

The potential impact of printer intrusions

Bogdan Botezatu, a senior e-threat analyst at Bitdefender, said printers present the largest potential security hole. "We get a lot of telemetry in our vulnerability assessment labs. The router is no longer the worst device on the internet. It's now the printer," he told The Register, a global online tech publication. The problem, he noted, is that printers offer "public shares that are visible to the internet."[6]

That visibility can have profound effects on your business. With a single unsecured printer, you could be leaving your entire network of connected devices vulnerable to attack, giving hackers the ability to spy on your networked devices—and compromising the security of your whole network.

We've all seen the effects of security breaches. In the XXX survey, respondents said the biggest impacts are increased help desk calls and support time, reduced productivity, and increased system downtime.

But a printer breach can be even more severe than that, particularly if you use a multifunction printer capable of storing printed data electronically. Print jobs stored to the printer's cache make it possible for hackers to gain access to sensitive personal or business information, including Social Security numbers, financial information, or internal memos and documents.

That is stolen information that can be used by your competition or that can cause serious harm to your company's reputation.

The easy solution: built-in security features

Clearly, companies need to address security even with their printers. And, really, doing so shouldn't be as hard as it sometimes is getting your documents to actually print.

Many of today's modern enterprise-level printers feature easy-to-use, built-in security that combats threats to your printers. These include:

- Automatic attack detection, protection, and healing
- Tracking use to prevent unauthorized use
- Simple sign-in options such as PIN or smartcards
- A proximity card reader that lets users quickly authenticate and print securely at a printer using their identification badge
- Secure encrypted printing for sensitive documents

When considering your next printer, whether desktop or multifunction, investigate the integrated security safeguards—and be sure to activate them. With simple, printer-specific features like those, there's no reason to remain vulnerable through your printers; after all, with the Internet of Things, there are plenty of other access points to worry about. Your printers don't have to be one of them.