SECURING YOUR PRINTER FLEET

A STRATEGIC APPROACH TO DATA SECURITY FOR YOUR ISSUANCE OPERATIONS

By Connell Smith, Vice President, Distributed Issuance and Supplies Product Management and
Mark Ruchie, Chief Information Security Officer

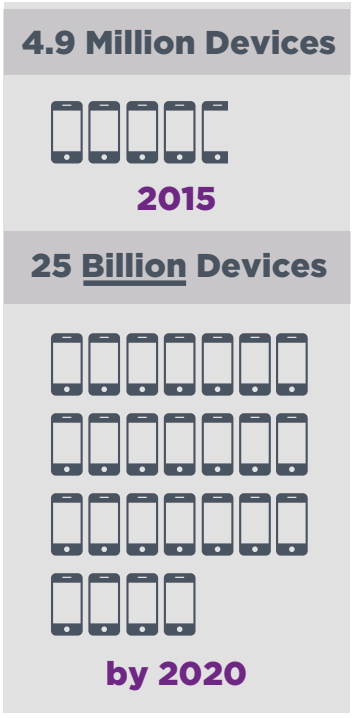
Entrust Datacard™

THE GROWING CONCERN OF CYBER SECURITY

Over the last year, it seems you can hardly go more than a week without seeing a headline about another major cyber attack. From large national retailers to health insurance companies and government entities, big-name organizations get the news ink, but the accelerating trend of cybercrime and data breaches is affecting organizations of all sizes and in every industry. A recent Experian survey found that nearly half of all organizations suffered at least one security incident in the last 12 months[1], with overall cybersecurity incidents increasing 38 percent over 2014[2]. Not only are cyber security incidents becoming more common, they're growing more costly every day, with the average data breach now costing an organization $3.79 million, a 23 percent increase over the last two years.[3]

1. https://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf
2. http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html
3. https://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf

GROWTH OF THE INTERNET OF THINGS



Common Types of Cyber Attacks

The growing threat of cyber attacks comes in many forms. Two of the more familiar types are social engineering and brute force attacks. Social engineering attacks use tactics such as phishing (fraudulent-but-convincing email or other communication) to trick users into divulging information that allows access to secure systems. Brute force attacks use sophisticated password- and credential-hacking software to "crack" the security credentials of authorized users.

The various "wares" are also familiar cybercrime tools. Spyware, malware and the like run behind the scenes on a computer or network, covertly watching users' network activity and stealing secure credentials and sensitive information.

Another familiar type of cyber attack, denial-of-service (DoS), does not aim to obtain sensitive information, but rather shuts down an entire network. Though on the surface this type of attack seems less dangerous, as sensitive information is not compromised, a DoS attack can be equally devastating to an organization. Network and system downtime can create huge productivity losses, and the costs of identifying and removing the source of the DoS attack can quickly add to the monetary impact.

Perhaps one of the most severe types of attacks is a "man-in-the-middle" attack, where two people believe they are communicating directly, but a third-party is actually monitoring or altering communication between them. This can potentially expose data being communicated.

IoT Creates Myriad Vulnerabilities

The Internet of Things (IoT), a big-idea term that has been around for more than a decade, is now rapidly becoming a reality. According to Gartner, there are currently 4.9 billion connected devices that comprise the IoT, a 30 percent increase over 2014. Gartner predicts that number will grow to 25 billion devices by 2020, an almost 30-fold increase from 2009.[4] This vast ecosystem of connected devices creates a myriad of new vulnerabilities just waiting to be exploited by cybercriminals.

4. http://www.gartner.com/newsroom/id/2905717

SECURITY CONCERNS FOR CREDENTIAL ISSUANCE

Sophisticated cybercriminals are targeting new IoT devices, including specialized printing equipment such as that used for secure credential issuance.

Printers have been part of connected ecosystems for decades — even your basic desktop office printer is connected to an online server. Today, printers are becoming yet another attractive target for cybercriminals. A recent study showed that 63 percent of organizations have suffered a print-related data breach.[5] But sophisticated cybercriminals aren't only going after your basic desktop printer. They're increasingly targeting specialized printing operations, such as those for secure credential issuance.

For organizations with credential issuance operations — including financial card issuance, secure ID issuance, and credential issuance for the enterprise and healthcare worlds — the impact of a breach to the secure printing environment could be disastrous. The danger of compromised sensitive issuance data from a financial card or secure ID operation is clear, but these attacks don't just target the information transmitted to a printer. A cybercriminal can potentially leverage a "hacked" printer to gain access to other databases and networks, compromising more sensitive information. A print-related breach could also lead to a DoS attack that shuts down an entire issuance operation for an extended period of time, an equally devastating threat.

5. http://www.nuance.co.uk/landing-pages/imaging/quocirca/print-security-quocirca-whitepaper.pdf

CREATING A SECURE PRINT ENVIRONMENT

To combat this growing threat, credential issuers must look at the security of the entire printer environment — including all connected elements of both the physical and digital issuance and personalization ecosystem — and construct a map of all parts before developing a strategic plan to mitigate threats.

Physical Security

Securing the physical elements of the print environment requires securing facilities, employees, personalization software, supplies, card stock and the printers themselves. Securing an organization's facilities can seem rudimentary, but the range of technology is constantly expanding: alarms, locks, security cameras, identification badges and access cards all help control who can physically access the spaces of your issuance operation. It is also important to consider hours of operation, separation of duties between staff for appropriate checks and balances, which activities require multiple approvers, and logging of key activities. And, of course, any time human activity is required, it is important to provide proper screening and training to prevent internal threats or vulnerabilities to social engineering schemes.

Some credential personalization systems feature physical locks to prevent access to supplies or internal components of the personalization devices, as well as mechanisms for bolting down the device itself to prevent theft. Another valuable physical security measure is the secure storage and/or destruction of supplies that may contain sensitive information, such as print ribbon, embossing supplies, and failed or rejected cards. Not all organizations need the same level of security, so it is important to understand your unique risks and balance security against the need for cost-effective and efficient credential printing operations.

Digital Security

Securing the digital elements of your print environment begins with protecting the software applications used to issue credentials, manage printers in a fleet, manage inventory, or connect with other components of your digital ecosystem. Many traditional applications are likely already behind a firewall to limit access, but externally hosted solutions, i.e., "cloud" software, bring about new challenges in terms of access and network security. Secure authentication, i.e., login/password and multi-factor authentication protocol, provide a first line of defense against unauthorized access to applications, and verifying the identity of users. However, the devices in your ecosystem — the credential printers, computers, mobile devices, etc. — must also be authenticated, to prevent sophisticated cyber attacks wherein cybercriminals pose as seemingly legitimate devices to gain access to the entire print network and beyond.

Rapid Remediation: Identifying "Abnormal"

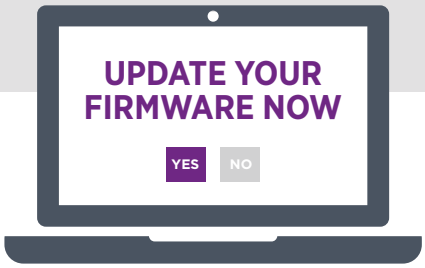
All of the above are tactics for preventing unauthorized access to your print environment. Unfortunately, even proactive security can't always prevent a print-related breach. In fact, many experts today believe that data breaches are now an unavoidable reality and that speed in identifying an attack and limiting its impact is the key to mitigating overall security risks. Thus, the second component of a print security strategy begins with understanding what is "normal," so that "abnormal" activity can quickly be isolated and neutralized. If your printer's IP address is used to connect an unauthorized laptop, would you know? Is the printer included in security scans? Do you keep the printer's firmware up to date?

The proactive side of breach remediation requires understanding the expected paths between users and systems, as well as between your print network and other elements of your connected ecosystem — and then defining which of these paths should remain unrestricted, which should be closely monitored, and which should be restricted. The reactive side includes checks and escalation paths to ensure rapid action when something is not normal. This is your opportunity to catch the smoke before it becomes a fire.

FIRMWARE UPDATES: A CRITICAL ELEMENT OF PRINTER SECURITY

You have likely received notifications that firmware updates are available for a digital device you use, from your phone to your watch to your music player. Firmware is software that manages and manipulates the data that drives these pieces of hardware, and firmware updates are a powerful way to add new functionality and improve performance without releasing a whole new version of the hardware. Your printer firmware is also regularly updated. Firmware updates often add new printer functionality for your existing hardware, enhance performance and throughput, and resolve reported issues. In addition, printer firmware updates contain critical updates to provide security features and address new security threats.

Maintaining up-to-date printer firmware must become a core component of both your printer maintenance protocol and your overall security strategy.



For example, in September of 2014, when the Shellshock vulnerability was exposed in millions of connected devices, Entrust Datacard took immediate action, releasing updated printer firmware to secure these identified vulnerabilities.

As cybercriminals grow more sophisticated, and with the growth of the IoT, new vulnerabilities and new cyber attack techniques are exposed regularly. Maintaining your print hardware means more than simply changing supplies and performing required cleaning. Maintaining up-to-date printer firmware must become a core component of both your printer maintenance protocol and your overall security strategy. By ensuring your print environment is using the latest printer firmware, you can help protect your printers against evolving threats, while ensuring optimal performance and efficiency.

WHAT YOU CAN DO

Prepare

- **Understand your threats.** In order to prevent a security breach, you must first understand all the different ways that your system can be compromised.
- **Create a map of your print environment.** Include all printer hardware, all software and devices connected to your print network, and how your print environment fits within your larger connected ecosystem.
- **Evaluate each element of your print environment.** Identify the security mechanisms currently in place, assess the adequacy of these mechanisms, and identify where additional security measures are necessary.
- **Create an action plan.** Develop a comprehensive plan for increasing security where necessary.
- **Define responsibilities.** It is important to have a clear understanding of who is responsible for ensuring that the appropriate measures are being taken to protect all sensitive information and assets. A newer role that has become more common is that of the Chief Information Security Officer (CISO). This individual works across the business and IT to prioritize these measures (a.k.a. security controls) based on measured risk and business context. For example, a CISO asks how a threat applies to the environment, how much a realized threat would impact business, and return on investment in security measures. Even so, ownership trickles down to all parts of an organization, from the CISO to the personalization system user and sometimes even to the card recipient themselves.

Perform

Once a plan is in place, it is time to implement any changes that are required. This means correlating events, monitoring and alerting, establishing processes, and planning for updates to systems or software throughout the infrastructure.

Seeking compliance with defined control standards and frameworks, such as ISO 27000 accreditation, can be helpful to ensure that appropriate measures are practiced and in place across the entire organization. ISO 27000 is a business accreditation that an organization is competent at protecting confidentiality, integrity and availability of business services.

Sustain

As discussed, security threats are constantly evolving and effective security efforts must evolve with them. An important step is prioritizing the regular firmware updates for your printer hardware. This will keep you at the leading edge of security for your print environment. Regularly conducting re-assessments of the security of your print environment will help identify new vulnerabilities before they turn into breaches.

Maintaining up-to-date firmware should be a core component of your security strategy, helping to protect your printers against evolving threats, while ensuring optimal performance and efficiency.

HOW ENTRUST DATACARD CAN HELP

At Entrust Datacard, we are committed to ensuring trusted identities and secure transactions for our credential issuance customers and their end users. As part of this commitment, our security experts are constantly monitoring threats and developing new security measures to keep our printer hardware one step ahead of cybercriminals. We regularly release printer firmware and driver updates that provide these powerful security features — including printer locks and alerts, enhanced security logs, encryption, digital certificates, communication configurations and updated networking components — as well as new functionality and enhancements to drive print productivity. These firmware updates provide our customers with ongoing investment protection, ensuring that their Datacard printer hardware continues to deliver outstanding performance while maintaining exceptional security.

Entrust Datacard also offers a complete portfolio of authentication and credentialing solutions that help our customers enact optimal physical and logical security — in their print environments and across the entire organization.

UPDATE YOUR PRINTER FIRMWARE NOW

Your free Datacard® card printer firmware update maintains your operational security and prepares you to respond to tomorrow's challenges — at no cost to you.

- **Elevate Your Printer Security:** Your card printers could be a prime target for sophisticated cyber attacks. Keeping your firmware updated reinforces the security of your printer environment, mitigating the risk of sensitive data leakage and preventing costly downtime from increasingly common denial-of-service attacks.
- **Boost Your Operational Performance:** Give your issuance operations a leading-edge advantage with access to enhanced printer capabilities, improved processing and compatibility with new advanced ribbons and supplies.

Contact Your Trusted Advisor For More Information

Phone: +1 952 933 1223
info@entrustdatacard.com
Visit Datacard.com/InFocus to update today.

Entrust Datacard™