Service

IT security for print shops.

HEIDELBERG

Foreword

This white paper focuses on the unique IT issues and solutions within a printing facility. Printers are becoming more vulnerable to security threats due to the adoption of increasingly complex IT infrastructures and information processes that expose information security gaps.

Cyber attacks have continued to double each year and new threats appear every day. Backup and data protection are not always a top priority for printers, but once job data loss, significant production downtime due to accidental data deletion, hardware failure, lost or stolen removable media, or a natural disaster occurs, it quickly becomes a top priority. They want to ensure that it never happens again and, if it should, that data loss or production downtime is minimized.

The same holds true when it comes to security. It is often low on the list of priorities. As with data loss, once printers have a computer virus infestation or have their production network hacked, emphasis on protection and prevention rises quickly to the forefront. There is one major difference between backup/data protection and security/privacy. With backup/data protection, the printer is often not fully aware of the specific risks and the costs incurred with a data/production loss. With security/privacy, printers do not see themselves as potential targets for an attack since they are not seen as an entity that stores important personal and financial information (i. e. a bank, government agency, hospital, or retail chain). The reality is no person or company is immune to potential threats.

One reason for backup and security being inadequate is that printers typically do not have IT staff on-site that are responsible for ensuring plant security, keeping employee/customer information private, and keeping the production running smoothly through the ever-changing threat landscape.

So, how do you ensure that security gets the required attention? The first step is to view security as a competitive advantage and not as an unnecessary cost. If your competitors are not using industry-standard and vendor-recommended “best practices” for securing their plants, then the print buyers who do business with them absorb unnecessary and unknown risks associated with that.

Eugene F. O’Brien, Senior Technical Support Analyst, Prinect® and CtP Services, Heidelberg® USA, Inc.

Eugene F. O’Brien

Eugene F. O’Brien is a Senior Technical Support Analyst at Heidelberg USA, Inc. focusing on internet infrastructure for the print shop. Eugene has worked in the printing industry for over 35 years starting as an apprentice at a “hot metal” typographer in NYC in 1975. During his time at Heidelberg, he has achieved his Cisco Certified Network Associate, Microsoft Certified Professional in networking, IBM Certified Specialist on PC hardware, and was certified by Data General on their UNIX operating system.

eugene.obrien@heidelberg.com
or phone +1 770 794-6205

Content


HEIDELBERG

Understanding the ever-changing threat landscape.

Printers, like any business, need to pay attention to what is going on in mainstream computing in this brave new world of business-to-business (B2B) and business-to-consumer (B2C) eCommerce. The outlined terms provide greater understanding of the ever-changing threat landscape.

PDF exploits

According to McAfee[1] and Symantec[2], nearly 50 % of browser-based attacks are PDF-based attacks. This should be of particular interest to printers who deal frequently with PDFs in their workflows. Adobe feels the solution lies with the new feature within Adobe Acrobat that silently updates the software as well as within its "protected mode." In protected mode, enabled by default, all operations required to display the PDF file run in a reduced-privileged level called "the sandbox". To perform an operation not permitted in "the sandbox", such as launching an attachment inside a PDF file using an external application (i. e. Microsoft Word), requests are funneled through a broker process. This process, which has strict policies for permitted actions, prevents access to potentially dangerous files. Adobe plans to incorporate "the sandbox" into Adobe Flash (another frequent target). Prinect Portal from Heidelberg allows an alternative to deal with Acrobat/PDF in the remote approval workflow.

Clickjacking

Clickjacking, also known as UI redressing, is an exploit that tricks users by displaying a dummy web page over a transparent web page. When users click a button thinking they are on the dummy page, they are actually clicking a button on the transparent web page underneath. This is a common technique used to get users to share private information.

SQL injection

SQL Injection happens when malicious code is inserted into variables that store user input for an SQL database. These databases are typically underlying components of a website, and the intent is to steal information such as credit card numbers. Generally, this is a result of bad practice in the SQL programming and can be avoided. Often, it is caused by failure to keep current with critical security updates – it is vital to have both OS security patches AND application service pack hotfixes up to date.

Cross-site scripting (XSS)

Cross-Site Scripting is a vulnerability typically found in web applications. There are potential risks for printers that host websites as well as for when their employees visit websites. XSS allows the attacker to inject client-side scripts into web pages viewed by other users. These scripts can then be used by attackers to bypass the access controls built-into that web site. This vulnerability implies that improvements to the infrastructure are needed.

[1] https://www.mcafee.com/tw/resources/solution-briefs/sb-browser-network-attack-methods.pdf
[2] https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

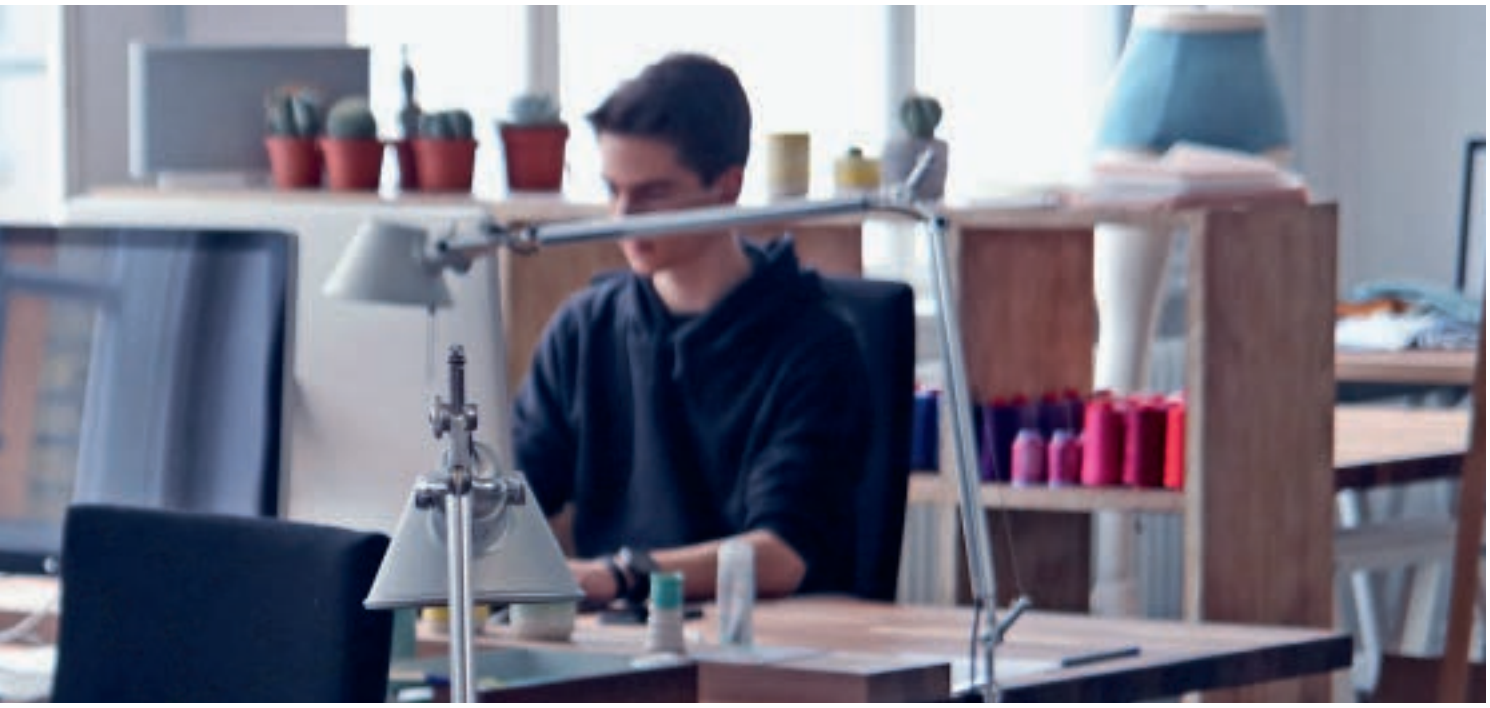
Malware

Malware or malicious software, is a catch-all for computer worms, Trojan horses, worms, rootkits, botnets, adware, ransomware, etc. that installs unwanted software on your computer. This could have a wide-variety of effects: slowed performance, computer malfunction, unwanted website redirection, or even identity theft. Malware has become the vehicle of choice for organized crime on the Internet. Stuxnet, an increasingly more popular version of malware, targets industrial software, particularly utility and electrical power plants. Relatively new "memory scraping malware" captures data from volatile memory within a system in order to circumvent encryption controls. It captures the data in memory where it must be decrypted to be read and processed. Other popular techniques used are fake antivirus warning pop-ups, fake software updates, or electronic survey scams.

Phishing

Phishing attempts to collect sensitive information by masquerading as legitimate e-mails or websites from legitimate companies like banks. A variation known as spearphishing has been listed by the FBI[3] as one of the fastest rising cyber threats. Unlike phishing, which targets random people, spearphishing targets specific interest groups, usually identified based on information that exists on Facebook, MySpace, blogs or forums.

[3] http://www.fbi.gov/news/stories/2009/april/spearphishing_040109



Spam

Spam, sometimes called “junk mail,” is the term applied to unsolicited bulk e-mail. Since this tactic is low cost and there are few methods to stop it, spam continues to be popular. The largest issue with spam is it consumes valuable bandwidth and disk space. Typically, spam filtering software and/or hardware are used to “whitelist” known good sources to permit that mail, and conversely “blacklist” known bad sources to block them.

SEO poisoning

SEO (Search Engine Optimization) poisoning, also known as Black Hat SEO, is when the results of search engines such as Google or Bing are poisoned to direct traffic to a rogue site. Legitimate companies also use SEO to increase their position in search engine results since users typically do not go past the first page or two. Hackers hijack these to get users to bad sites to steal personal information or install malware. Infected search results continue to rise from year to year.

Geotracking

A common security mistake people make every day is not realizing how much information they are actually sharing when they post pictures on the Internet. Most smartphones and some digital cameras can add the coordinates where a picture was taken. Pictures may contain the exact coordinates someone needs to find the location. This means that burglars and stalkers have new tools to help in their pursuit of their victims. To maintain privacy, ensure any cameras have “geotracking” turned off.

Whistleblowing sites

In reaction to WikiLeaks, new sites are expected to pop up targeting not only government organizations but now commercial businesses and industries – exposing company secrets, both good and bad, to the public.

Common IT myths & security lapses.

Myths	Facts
"Apple computers are not vulnerable to viruses or hackers."	While Apple[4] operating systems do not get the volume of attacks that Microsoft operating systems do, no computer is immune. Viruses such as OSX/Pinhead-B and Boonana trojan target Macs by monitoring browser activity in an attempt to get Facebook users to install malware. Apple does maintain their own security updates, which demonstrates that they are susceptible to vulnerabilities and attacks
"We are just a small printer and hackers are not targeting us."	The Wall Street Journal[5] reported a huge increase in hacker attacks on small businesses. Many small businesses simply do not have the resources to protect themselves or to recover. According to the latest figures 20 % of printers do not use antivirus software, 60 % do not use encryption on wireless links, and 66 % have no security plan in place. With a majority of printers leaving themselves vulnerable to attack, it should be no surprise that hackers would consider them easy targets.
"I have nothing a hacker would want."	Hackers can harvest information such as customer lists (containing contact or credit card information), employee databases (including social security numbers) to potentially advertise confidential customer information. In addition to hackers, others such as disgruntled ex-employees may have motives and important access information as well.
"We are protected by a firewall."	A firewall protects the perimeter from breaches only if the software is up-to-date and the rules are correctly defined. It does not protect against internal threats including threats from removable media like a USB drive or CD/DVD, or threats from a dangerous link or e-mail attachment. Additional steps such as upgrading to next-generation unified threat management (UTM) devices with deep packet inspection, content filtering intrusion protection systems (IPS) and gateway antivirus are advised.

[4] http://support.apple.com/kb/ht1222

[5] http://online.wsj.com/article/SB10001424052748703483604574630690362605018.html?mod=dist_smartbrief
http://blogs.wsj.com/tech-europe/2011/03/21/hacker-threat-to-business-increasing/
http://online.wsj.com/article/SB10001424052748704398804575071103834150536.html

During the course of customer site visits for installations, upgrades and service, or support calls into our help desk, Heidelberg consistently encounters a common thread of IT security deficiencies.

Poor password policy

Passwords not defined in an "acceptable use policy" are often left vulnerable to attacks. Common password gaps include:

- For network appliances like firewalls, switches, routers, wireless access points, etc., printers tend to still use the default password from the vendor. Such passwords are well known to hackers and can be easily found in product documentation or through a simple search engine – leaving all confidential information vulnerable.
- User passwords on servers and workstations are non-existent or simply too easy to guess (for example, using "password" as your password, or "123456"), or they are written on notes attached to the device.
- Passwords are unknown. When attempting to get into a device to look at the configuration to resolve an issue, no one in the plant knows what the password is because it is old or the password originator has left the company.

Poor internet infrastructure

There are three aspects to internet usage at a typical printing plant:

- General web surfing and e-mail by employees
- Remote service provided by vendors such as Heidelberg
- Uploads/downloads/softproofing/digital approvals by print buyers

Lack of anti virus protection

Many printers do not run antivirus software on workflow equipment. The potential for viruses is not only from the Internet but from inserting a USB drive or CD/DVD.

Poor network infrastructure

The ideal network infrastructure should perform well and be reliable while protecting your business. It is important to avoid the "egg shell theory" where the perimeter is protected with a hard shell but everything inside is still very loose. Common mistakes include:

- Use of network equipment designed for personal home use not commercial equipment designed for a business
- Use of obsolete equipment at vendor's end of life that is no longer under warranty nor has current security updates to protect against new threats
- Protecting the infrastructure equipment on a UPS (uninterruptible power supply) with battery backup
  A small spike or brown-out can bring down the network temporarily causing disruption to production while equipment is rebooting
- Firmware in the equipment is not kept up-to-date so critical security updates that fix holes that a hacker can exploit are not patched
- Configurations are not hardened according to industry-accepted and vendor-recommended standards
- Wireless implementations are very unsecure, "rogue access points" lack encryption, have dated firmware, and use default passwords, which leaves the wireless LAN very vulnerable to stolen internet connection

What should a printer do?

Every printer should take security and privacy seriously. Printers need to take a proactive approach to their company's IT security, rather than a reactive one to ensure their business is protected. Knowledge is the best defense to fend off unknown threats from the outside or inside their company.

Assign a chief security officer

A good first step is to assign someone in the organization to be the chief security officer (CSO), the person responsible for establishing the policies and procedures that the entire print shop should follow to help limit exposure and liability. This person will be the driver for security in the print shop involved in the decision-making process as well as administrating an incident response team (IRT). The IRT will investigate, document and resolve any suspected breaches or other reports of issues.

Vulnerability assessment

Conducting a vulnerability assessment is another good step in identifying areas that need to be addressed. This should be conducted by an independent source rather than doing it internally. Heidelberg USA offers Prinect Security Analysis® where we will visit your plant and identify any problems that exist as well as make recommendations on how to eliminate these problems. If desired, we can also implement the recommendations.

Acceptable use policy

Establish an acceptable use policy. Employees, as well as visiting customers and vendors, rely on the Internet for accessing regular services and information. In order to leverage the full scope of the Internet without its drawbacks, printers need to effectively manage and minimize the potential threats. Careful consideration must be given to questions such as who should have access, what they should have access to, and with what restrictions. An acceptable use policy is an important tool for managing access to the Internet. An effectively written policy will clarify the level of service that employees and visitors can expect, as well as provide a clear definition of the role the Internet will play in your business.

Remove unwanted software

Unwanted software is defined as software not installed by the current user. It often comes installed on computers purchased through stores or online. These programs should be removed whenever possible.

Harden servers, workstations, and printers

Follow the guidelines from vendors like Microsoft and Apple for hardening their operating systems and vendors like HP for hardening their printers/proofers.

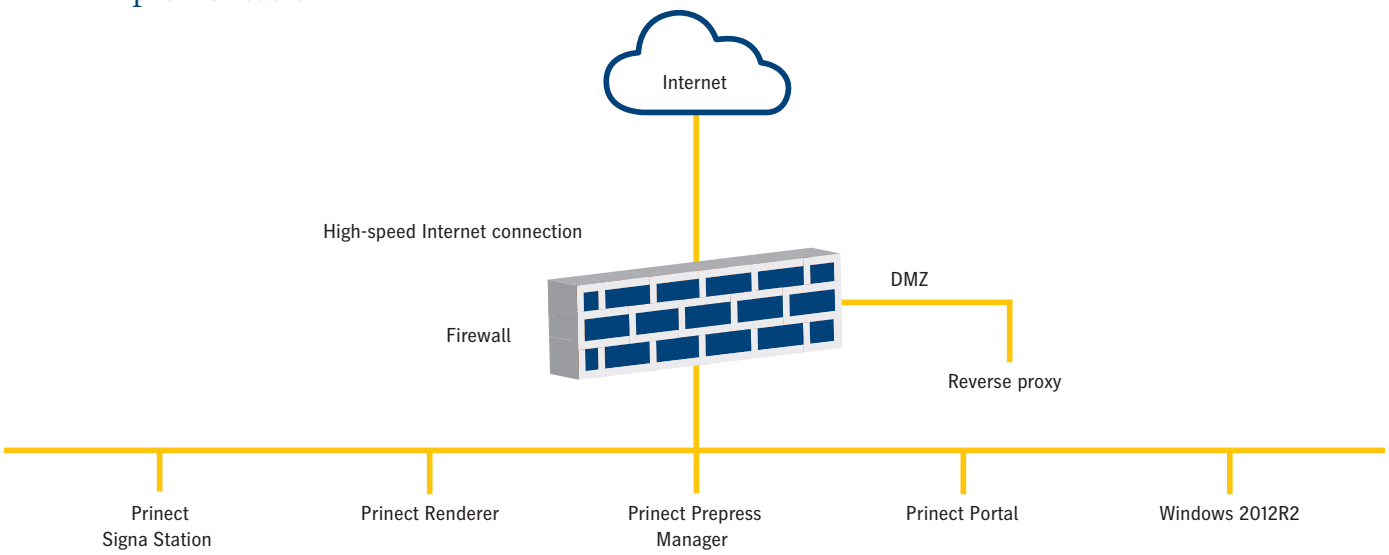
Install antivirus software

Not only is it important to run antivirus software, but also keep the software up-to-date and the definitions file up-to-date.

Standards compliance

If a printer accepts credit cards, they need to ensure their network and business is PCI (payment card industry) DSS (data security standard) compliant.

DMZ implementation



Eliminate FTP

FTP is still commonly used in print shops. The problem is FTP is based on software code from the 1980s and its deficiencies are well known by hackers; hence the nickname "Failure To Protect". If a printer accepts credit cards, they need to ensure their network and business is PCI (payment card industry) DSS (data security standard) compliant.

FTP poses many problems that firewalls do not handle:
- Additional TCP/IP connections are used for data transfers
- Data connections may be sent to random port numbers
- Data connections may originate from the server to the client, as well as originating from the client to the server
- Data connections' destination addresses are negotiated on the fly between the client and server over the channel used for the control connection

FTP does not encrypt login information:
- Prone to eavesdropping and theft of passwords or other sensitive information
- Possible to hijack connections

Anonymous FTP is truly anonymous:
- There is no record of who has requested what information

Modern solutions like Prinect Portal are integrated into the workflow and are more secure and reliable.

Implement DMZ and reverse proxy

When providing web services to print buyers, printers should provide a de-militarized zone (DMZ) and a reverse proxy.

Use full disk encryption (FDE) on mobile computers

Mobile computers like laptops can be lost or stolen. The data on that laptop could include sensitive information about print buyers or production employees as well as information about the network and servers such as passwords and network configuration.

Additional resources.

Utilize the websites below to get information on the latest threats and security tools.

Adobe security bulletins & advisories
https://helpx.adobe.com/security.html

Apple security updates
https://support.apple.com/en-us/HT201222

Cisco security advisories
https://tools.cisco.com/security/center/publicationListing.x

European Cybercrime Center
https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3

Flash Player security & privacy
https://www.adobe.com/devnet/security.html

McAfee Labs security advisories
http://www.mcafee.com/apps/mcafee-labs/signup.aspx?region=us

Oracle critical patch updates & security alerts
http://www.oracle.com/technetwork/topics/security/alerts-086861.html

Microsoft security advisories
https://technet.microsoft.com/en-us/security/advisories

SANS (SysAdmin, Audit, Network, Security)
http://www.sans.org/

Symantec security advisories
http://www.symantec.com/avcenter/security/SymantecAdvisories.html

US CERT (Computer Emergency Response Team)
http://www.us-cert.gov/

US Department of Justice
https://www.justice.gov/criminal-ccips/ccips-documents-and-reports

Summary.

Wherever possible, reducing and eliminating threats can ensure continuous production, thus making your business more reliable and profitable.

As print shops aggressively move forward to provide new internet-based services and products to their customers, they face increasing threats from hackers and viruses, spyware, adware, malware, etc. The cost to printers can rise exponentially based on the frequency and duration of each incident. While some security decisions are made on the front end of a purchase or installation, in reality, security requires an ongoing commitment and is ultimately the responsibility of each customer. Wherever possible, reducing and eliminating threats can ensure continuous production, thus making your business more reliable and profitable. The best way to survive an attack is to be prepared for it.

Each business has a responsibility to evaluate their security risks and decide upon the security practices that they will implement. Whether an attack is intentional or accidental, internal or external, it impacts production and ultimately costs the company money. Network breaches continue to increase and now it is not always clear that a compromise has been made to a company. Today, new laws are being created to prevent attacks but may also place restrictions on businesses. In 2011, a new data breach notification law, DATA (Data Accountability and Trust Act) – HR 2221, changed business processes including those used at printers. With growing threats and increased regulations, every employee, from bottom to the top, needs to be vigilant in computer and network security. The goal is to minimize vulnerability and secure the production network.

Heidelberger Druckmaschinen AG
Kurfuersten-Anlage 52–60
69115 Heidelberg
Germany
Phone +49 6221 92-00
Fax +49 6221 92-6999
heidelberg.com