Building End-to-End Data Security into Inkjet Print Operations

January 2018

An Inkjet Insight White Paper for Inkjet Professionals
Commissioned by Crawford Technologies, Inc.

Building End-to-End Data Security into Inkjet Print Operations

By Elizabeth Gooding

January 2018

Table of Contents

Introduction

The issue of data security is so pervasive that it has moved from an IT and boardroom discussion to become the topic of movies and television shows. More than 7 billion records were exposed through breaches in just the first nine months of 2017, a jump of over 300 percent from the prior year. Five of the top breaches in 2017 were among the largest ten breaches of all time.[i] With over five million records lost or stolen every day, protecting businesses and consumers from data breaches is a top concern among executives in all industries. While there is a tendency to think of data breaches in terms of the web and digital initiatives, security is no less critical for printing operations.

Printing organizations, particularly in-plant operations within financial services and healthcare organizations, can be targets in their own right, or simply points of entry for hackers to gain access to the corporate network. Over half (52%) of breaches in the United States were due to hackers and criminal insiders,[ii] however 49% of companies surveyed by Ponemon Institute in 2016 acknowledged a data breach caused by a third-party vendor that resulted in the misuse of sensitive or confidential information and another 16% were not certain that such an event had not occurred.[iii] This gives print buyers a great deal of concern about the data security of their suppliers and should, in turn, make printing organizations take careful account of the security procedures of their own business partners.

7 billion+ records exposed
300% escalation
5 of the 10 largest breaches

Source: 2017 Cost of Data Breach Study Ponemon Institute

The Cost of Data Breaches

The costs of data breaches are escalating with the average per capita cost of a data breach reaching $225 in the US[iv]. This represents the aggregated costs for the immediate discovery and response to the data breach, including forensics and investigations, and efforts following discovery and investigation, such as the notification of affected individuals, compensation, legal fees and potential fines. This means that a relatively small mailing list of less than 5,000 records that contains personal health or financial data, if breached could cost over a million dollars to remediate.

The nature of transaction and direct mail print operations, in particular, make them target-rich sources of personal data in high volume. However, as commercial printing operations begin to add data and personalization to their portfolios, they too can be targets. When companies are making a technology shift, such as a move to inkjet, there are factors that increase the potential for exposed data:

- Companies are using inkjet to expand into new markets, many of which require variable data;
- Firms without prior data-handling experience are adding data science and personalization capabilities;
- Enabling inkjet productivity requires a variety of supporting software to optimize the production flow including data transformations, sorting, splitting and merging of files;
- There may be new dynamic composition, postal automation and color management software as part of the overall solution;
- New servers may be needed to accommodate software and data management;
- Some software products may be implemented as cloud solutions introducing an additional source of vulnerability;

In general, a transition to inkjet represents a significant operational change, and change is a breeding ground for risk. Recognizing the potential for risk means that change can also be an opportunity to embed security measures into the end-to-end process design for the inkjet implementation.

Planning for End-to-End Security

Building security into the complete print production process must consider every step from implementation and ongoing maintenance through production management and business continuity. Consider every aspect of the process where data could be potentially exposed:

- System Configuration
- Customer Ordering
- File Transfer
- Print Quality Testing
- Software Testing
- Application Testing
- Production Proofing
- Production Processing
- Archive/Reprint
- Equipment Retirement

At the front-end of the process, it is important that systems are configured properly. Many recent data breaches have been enabled by improperly configured cloud and in-house security protocols. Web-to-Print Systems are particularly vulnerable and should be reviewed carefully during configuration and every time a software upgrade is installed. In general, if a device or service is not intended to access the network, disable the relevant ports or settings. It doesn't help to have great locks if you don't close the door. In 2016, misconfigured websites and databases allowed the exposure of over 256 million records.[v]

For example, St. Joseph Health (SJH) of California exposed patient information online after installing a new server. A feature of the new server was a built-in file sharing application for which the default setting allowed public access. SJH failed to examine or modify the default settings and, as a result, the public had open access to personal health information for over 31,000 SJH patients. SJH agreed to pay a $2.14 million fine and agreed to implement a corrective action plan to help prevent similar situations from occurring again.[vi]

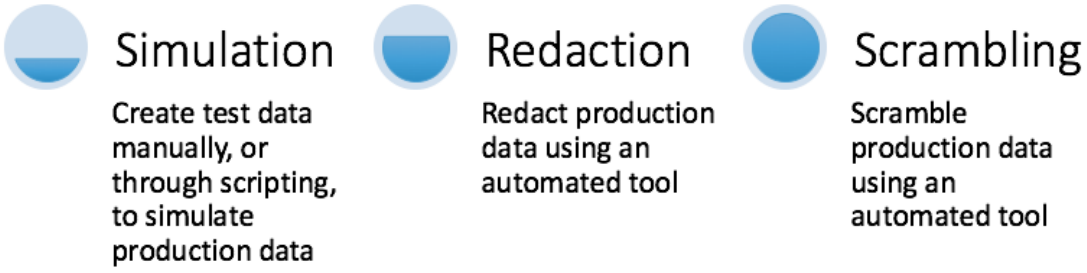
At the back end of the process, when equipment is relocated or retired as part of the decommissioning process, ensure that data is wiped from all temporary and disc storage and that the data is overwritten to ensure it is not reachable by a knowledgeable hacker.

Security planning and governance must consider physical device security for any components of the solution that access the network or the web such as digital front-ends, print operator consoles and camera systems. Data should be encrypted both at rest and in flight, however, in a print environment the data must eventually be imaged onto paper in human readable form. That makes the technical and physical challenges of maintaining security in a print environment unique.

Challenges with Securing High-Speed Printing

Printing environments have a lot of moving parts, literally, and these parts need to be seamlessly integrated. Data is processed, formatted and printed. The printed output may be cut, perforated, bound or folded and perhaps inserted into an envelope. These processes are often controlled by barcodes that track the production process from step to step and also track an individual item or mail piece. They must ensure that data is not printed on the wrong page and that pages are not inserted in the wrong envelope. In the case of checks, they must ensure that a check is only printed once, printed on the proper form and, in cases of production errors or inventory obsolescence, that materials are destroyed in a secure manner.

Once in production, these measures are an important layer of security in protecting personal data and preventing fraud. However, getting these systems into production requires access to test data. There are three ways to generate test data:



Generating a useful volume of test data that is representative of the production data can be expensive and time consuming. As changes are made to an application, new data may be required. Even after creating a robust suite of test data, this approach may not capture all potential scenarios found in production. In cases of a production failure, the simulated test data may not be able to replicate the failure. In that situation, a company is faced with two bad options: fail to deliver on Service Level Agreements or violate their data privacy agreements by sending production data to outside partners in order to diagnose the problem in a timely fashion. Another option is to send redacted production data.

Redaction refers to the practice of deleting or blacking-out fields of information. In some scenarios, redacting production data can be effective, for instance, when unit testing the print process as a stand-alone step. However, as soon as the testing process expands to include any connected or offline devices that require barcodes to operate, the redaction approach is no longer useful. When a data-point is removed from the document it needs to be removed from the whole document, including any data embedded in barcodes, metadata or human readable codes. Removing the data eliminates the ability to test the process from formatting through finishing and inserting. In addition, it limits the viability of proofing steps.

A more visibly accurate and functionally complete approach is to scramble production data. With the scrambling approach, data is rendered unusable in identifying personal information, yet remains completely functional for testing and proofing requirements. This approach has the benefit of providing robust test data during implementation and testing phases and also supports root cause analysis for production failures. Unlike the redaction scenario, all data necessary for integration testing using barcodes or metadata is present. If failures occur during production, the actual production file where problems occurred can be sent to third parties for analysis if the personal information is first scrambled. Finally, data scrambling can also be used to satisfy requirements for de-identification under current HIPAA regulations, if data is to be further analyzed for research purposes once rendered not "personally identifiable."

Best Practices: Data Protection by Design and by Default

"Data Protection by Design and by Default" originally introduced in Canada in the 1990s and more recently formalized within the General Data Protection Regulation (GDPR) in the European Union, but its intent is widely present in US data privacy regulation as well. In essence, it means that for any system or process, use of personal data is limited to the purpose for which the data was collected and only those people necessary to access personal data can do so.

To ensure data privacy in a print environment, protection must be built into the technology infrastructure and business practices by default. Having tools to encrypt, mask, or scramble data is not enough if they are not used properly. Print processes should be designed from the start so that data is encrypted whenever possible and redacted or scrambled whenever encryption is not possible. These actions should be automated and not left to the discretion of a programmer or print operator.

To ensure data privacy in a print environment, protection must be built into the technology infrastructure and business practices by default.

Table 1 – Best Practices for End-to-End Production

Step	Protection
Receipt of data	• Encrypted transmission • Scan all incoming files for viruses
Storage of data	• Encrypt at rest • Automatically delete data at earliest compliant date
Data Transmission	• Encrypted transmission whether to internal or external location • Automatically redact or scramble when transmitting externally, except for production processing
System Testing	• Automatically redact or scramble data for all testing processes, internally and with outside partners
Production Failure	• Automatically scramble production files needed for third-party support of system failure.
Disaster Recovery Testing	• Use scrambled data for all testing prior to fail-over tests • Encrypt transmission
General	• Secure network access for all connected devices including DFEs, servers, operator consoles, camera systems and scanners. • Validate cloud security settings with a network security specialist • Disable all unnecessary ports and services to reduce vulnerability

1. In addition to securing data within the print operation, ask clients if the data that they are sending for testing purposes includes live customer information.

2. Discourage clients from sending production data for use in testing because reducing unnecessary exposure to personal data reduces the likelihood of loss.

3. If the client insists on the use of production data for testing, ensure that files are immediately scrambled on receipt.

Considerations for Production Inkjet Environments

The guidelines above are relevant in any production printing environment, but have special implications when standing up a new production inkjet solution. Security challenges begin during the inkjet evaluation phase when working with OEMs to evaluate print quality and to estimate the total cost of operating the solution.

When evaluating print quality, tests should be conducted using "fingerprint files" that exercise the boundary conditions of the device such as color gamut, color density, line density and text raggedness. They should also be conducted using a representation of current production work to ensure that the device and paper being tested can run all the way from print through finishing. In many cases a printer may deliver high quality output, however that output may not be "finishable." A range of problems can occur from paper being overly wetted to overly dried that will make the output incompatible at some stage of the finishing process. Testing finishing requires barcodes and barcodes require data.

Security challenges begin during the inkjet evaluation phase when working with OEMs to evaluate print quality and to estimate the total cost of operating the solution.

The other reason for using a representative sample of current production work is to estimate the relative ink consumption of different devices or different papers for a particular device. Ink is one of the major factors in estimating the total cost of ownership and can differ greatly between various device and paper combinations. Testing of ink consumption may initially be conducted with OEMS at their facility requiring data to be transmitted and subsequently in-house while testing papers. It is important to use files that are as close as possible to production to get good ink usage estimates. It is also important that production data not be used for this purpose. Redaction is not a good solution in these instances since it voids the barcodes, reduces ink usage and changes the appearance of the document. Data scrambling, unlike redaction, makes the process seamless and secure both during the data handling process and when hard copy is circulated for quality review internally and with suppliers and clients.

As noted earlier, technology transition is a time of great vulnerability with multiple vendors to coordinate and new protocols for employees to learn. There may be new composition, transformation or workflow software to be deployed and tested. Employees, client staff, vendor staff, and consultants may all be involved. Where there is confusion, there is opportunity for a breach. If a third party, such as a supplier or subcontractor, is involved in a data breach, the cost to remediate can increase by as much as $17 per compromised record.[vii]

Often there is great pressure to get the system implemented quickly – particularly if the transition necessitates production downtime. Creating a security protocol that ensures that all test data is scrambled data helps to ensure that live data will not inadvertently be sent to an outside vendor during the rush to production readiness.

In many inkjet implementations new software is implemented to comingle jobs from multiple customers in order to optimize production workflows. This underscores the need for functional barcodes during the testing process to track document integrity at the piece-level throughout the process.

Data scrambling makes the process seamless and secure both during the data handling process and when hard copy is circulated for quality review …

Multiple Benefits of End-to-End Data Protection

Implementing sound security policies and solutions can pay back in many ways. Naturally, making the environment more secure reduces the likelihood of breaches and all the negative implications of data loss. However, there is still the potential for a determined and malicious hacker to cause private data to be exposed. If this occurs, the strength of your security procedures and ability to demonstrate adherence to those procedures can greatly mitigate the impact of the breach.

In the case of HIPAA data privacy violation, a provider who is deemed negligent in their efforts to secure data will see substantially higher fines than an organization that can demonstrate secure processes, a culture of governance and an investment in ongoing employee training extending to the end-point of their interactions with third-party suppliers. The extensive use of encryption can reduce the cost of a breach by $16 per capita on average[viii], and it is reasonable to infer that the scrambling of data would have a similar impact.

Avoiding the designation of "negligent" is also critical in communicating the breach to customers. Customer churn is a major factor in the cost of a breach and the ability to demonstrate that data was protected is key to reducing churn. The ability to demonstrate a culture of security and automated processes for protecting data are also critical in attracting clients during the sales process and to maintaining the relationship.

When large volumes of production data can be scrambled to allow testing of multiple scenarios clients will benefit from a robust, seamless end-to end testing process and from being able to perform user acceptance testing without working with redacted test output.

- Reduce Chance of Breach
- Mitigate $ Impact of Breach
- Avoid Designation as "Negligent"
- Lower Insurance Costs
- Improve Customer Perception
- Provide More Robust Test Process
- Enable Realistic Cost Calculations

Production operations benefit from the ability to perform realistic calculations of operating costs on equipment and software without fear of compromising data.

While the purchase of cyber and data breach insurance can help manage the financial consequences of an incident the ability to obtain coverage and the cost of that coverage will also be impacted by the ability to demonstrate strong preventative measures.

The level to which a company implements sound security policies and solutions is one of the most critical factors in maintaining a viable organization. With clients contractually leveraging suppliers to take on a greater share of the risk of losses due to cyber attacks, a failure to invest in security solutions could bankrupt the organization in the event of a breach.

When planning a production inkjet implementation, take the opportunity to identify security gaps and plug the holes. Question all suppliers about their own protocols and ensure that all precautions are taken to harden devices and prevent access. Document your efforts and use your security investments to open up new and lucrative opportunities with clients who value security minded partners.

About Inkjet Insight

Inkjet Insight LLC is the most complete, unbiased and valuable source of information for companies evaluating and using production inkjet.
For more information visit www.inkjetinsight.com

For analyst or speaker inquiries, contact info@inkjetinsight.com

Follow us on Twitter: @InkjetInsight

End Notes

[i] Source: Risk Based Security Q3 2017 Data Breach QuickView Report

[ii] Source: 2017 Cost of Data Breach Study Ponemon Institute

[iii] Source: Data Risk in the Third-Party Ecosystem Ponemon Institute 2016

[iv] Source: 2017 Cost of Data Breach Study Ponemon Institute

[v] Data Breach QuickView Report 2016 Data Breach Trends – Year In Review Sponsored by: Risk Based Security Issued in January 2017

[vi] http://www.channelfutures.com/msp-501/botched-server-install-results-214-million-hipaa-breach-fine

[vii] Source: 2017 Cost of Data Breach Study Ponemon Institute

[viii] Source: 2017 Cost of Data Breach Study Ponemon Institute