# Cyber Safe Production Workflow

**Aaron Hale**
is a senior advisor for Canon Solutions America's Enterprise Services & Solutions division. With 20+ years' experience in the corporate enterprise, SMB and graphic communications industries, his passion is to help leaders of all types make strategic business decisions in their go-to-market and operational directions and then move them into actionable programs. Aaron can be reached at ahale@csa.canon.com

## Maintaining a secure environment is not just an office or IT network issue in today's volatile business world. It's essential in every department of an organization, including the print center.

Sustaining your print center's value proposition goes beyond on-time delivery, economical services, high quality and fast turnaround. An in-plant team that contributes to the greater good of the parent organization is a team that garners loyalty when the chips are down and is perceived as a solid investment. Of course, as a manager you have a fiduciary responsibility to engage in routine benchmarking and cost management, demonstrating responsible business practices, but is that where your responsibilities end?

Do you have too much to do? Of course you do. Could there possibly be more? Sorry, but the answer is yes — and maintaining a secure production environment is probably one of the most important areas of heavy lifting that you might be asked to take ownership of.

A secure production and office workflow is defined as having stable and resilient processes with redundancy, process controls and a disaster recovery plan in place. For in-house print operations, these disciplines help to keep your parent organization compliant with regulatory obligations and if sustained, can add another dimension to the value your operation provides your administration.

If you haven't already, it's a good idea to discuss your organization's regulatory compliance obligations with your administration and any security policies in place that need to be monitored and enforced. It might also be a good idea to bring up the subject of attestation to ensure a consistent state of compliance. Attestation, by definition, is the act of providing evidence that something is true.

There are industry standards and methods of validation by accredited third parties, and for print service providers the most widely accepted is the Statement on Standards for Attestation Engagements (SSAE-16) certification. In a future issue I will elaborate in more detail on this point.

If your operation actively engages in insourcing, having an SSAE-16 certification can help expand opportunities to service customers that require highly confidential print or scanning work. This can also apply to in-house departments that currently outsource the same type of work to a provider that has such stringent security measures and controls in place.

### Risk Mitigation

There are certainly other areas of risk mitigation opportunities such as using SFTP (Secure File Transfer Protocol) rather than the unsecured FTP (File Transfer Protocol) for moving customer files around. This helps to protect data in transit, and you could employ a PGP type of encryption for your data at rest. Most Web-to-print and MIS solutions today utilize Secure Socket Layer (SSL) transport protocol for data and print stream movement as well as file encryption on digital front end (DFE) hard disk drives (HDDs).

Similar to the best practices of hardening devices connected to the internet or a larger WAN (wide area network) in fleet environments, production devices and/or DFEs that are connected in kind must also be protected (see *IPG* June article: "Can a Data Breach Sink Your Fleet?").

In many cases production devices are not connected to the internet or larger organization WAN and in the case of in-plant facilities may be on a separate subnet of the parent organization network and not exposed to outside threats. However the rule of thumb of "if you are not using it, turn it off" applies here, so just disable any unnecessary ports.

Additionally, DFEs and workflow software workstation and server host CPUs should be patched routinely by updating their respective operating systems (Windows, Linux, UNIX, etc.). Remember that the victims of recent ransomware attacks could have been spared simply by having updated and patched their operating systems in a timely fashion.

## Threat Assessment

We all know that by implementing Web-to-print and/or management information systems (MIS), the bar can be raised in terms of maximum efficiency, productivity and accountability, but it can also be a point of risk exposure. Ask your vendors or product manufacturers if their offering has undergone a third-party threat assessment. If so, ask them for a current report, especially if you are vetting a new cloud-based system provider.

**Maintaining a secure production environment is probably one of the most important areas of heavy lifting that you might be asked to take ownership of.**

Finally, controlling access and monitoring print activity of key operators and other staff is critical. Consider operating on a "need to access" basis. In other words, a prepress person or secondary key operator should not have access permissions to specific sensitive client or department files and print jobs. Be meticulous about this, and during your monthly reporting include an audit of user and printer activity to validate the effectiveness of the controls that you put into place.

So, is there such a thing as a cyber secure production workflow? You bet there is, when you employ due care and due diligence with proper applications and policies. You just might find that it will save your organization a bundle. Maybe not today or tomorrow, but if you are paying attention to the state of our cyber world, it could be a "when" not "if" scenario. ***IPG***