Beyond the firewall

Canon Solutions America's Pete Kowalczuk on why you must protect your data now

Nobody is safe. When it comes to cybersecurity, that's the message Pete Kowalczuk wants you to walk away with. In what is one of the biggest hot-button issues for today's owners of businesses of all sizes, protecting your company's data is critical. Ask Kowalczuk, president of Canon Solutions America, Inc., and he'll tell you that security is your be-all, end-all priority.

Want proof? According to research by Risk Based Security, there were more than 5,000 publicly disclosed data breaches in 2017 with 7.8 billion records disclosed. Dubbed the "Year of the Data Breach," 2017 was the worst ever regarding frequency and severity.

The future isn't any brighter. The Ponemon Institute's "2018 Study on Global Megatrends in Cybersecurity" shows that 67 percent of 1,100 senior information technology practitioners surveyed around the world believe they're at risk of cyber extortion.

CANVAS sat down with Kowalczuk to get his thoughts on why today's printers should be on alert and how they can protect what matters to them the most.

Pete Kowalczuk

What should every printer know about cybersecurity?

That it goes beyond the normal office environment. A common misconception is that a digital print operation is immune from attack because it's positioned behind a firewall. This is not true. Print operations, in-plant and commercial printers have the same risks as any other business—if not more. Printers can receive files from a variety of users via myriad file sharing methods (email, USB drive, FTP, etc.). This can expose you to more risk if the proper precautions are not taken. You must view security through the same lens as any group that cares about safeguarding their data (or their customer's data) and the protection of their operation.

Are today's printers taking the proper precautions?

While there are some that have recognized the need for cybersecurity in their operations, these are often ones that serve customers in regulated industries—and may have been steered in that direction by them. Others maintain the status quo of the misconception we just discussed. This false sense of security can expose their organization to significant risk. Cybercriminals will target anything that can help them make money. Printers are not immune. With the average security breach cost in the U.S. of $7.35 million, it only takes one to put you out of business.

Why are risk management and threat mitigation key strategic elements for building an effective security framework?

Because it's nearly impossible to be 100 percent cyber secure. To effectively compete in today's business climate, organizations are integrating more technology into their business processes, which enables users to be more connected than ever. But in doing so, it increases their risk and threat exposure.

Given this reality, organizations fall into three camps: Those that have been hacked and don't know it. Those that have been hacked and know it. And those that will be hacked. An effective security framework uses business drivers to guide considerations surrounding cyber risks. This should be an important part of your risk management processes. Threat mitigation is critical toward eliminating or reducing the potential or possibility of compromise.

What's the best way to get started?

Consult with a subject matter expert in cybersecurity. Begin with a security assessment of your operation. This could include a vulnerability assessment, risk assessment and a business impact assessment. From there, you'll get a better picture of where the potential gaps are in your security posture, as well as recommendations on how to mitigate the identified risks.

Why is security something printers must keep in step with?

Security is "a journey, not a destination." While there's no such thing as being 100 percent secure, due care and due diligence mitigate risks. Threats evolve on a daily basis, and cybercriminals are taking advantage of organizations that don't try to understand those risks. Security is not a box you can forget about after it's checked. Making it a normal part of your daily routine is the best way to mitigate the risks you face every day. It's table stakes in business today.

What best practices can printers employ to get the most from their investment?

Take steps to educate your staff on cyber etiquette, potential security risks and best practices with electronic communication. Monitor file submissions and data transfers. The USB drive has been the culprit of some of the most destructive cyberattacks in recent history. Set up a dedicated PC that is not connected to your network or the internet to first scan the USB for malware and, if necessary, sanitize it before moving the files into their system.

You should ensure that any type of web-to-print system uses file encryption in the movement of files and harden the receiving systems and your digital print controllers. If not already activated, enable the security features on connected office equipment and digital presses.

Finally, attestations such as a SOC 3 audit or ISO 27001 certification can set in motion more secure operational processes and ensure a level of consistency in your security posture.

How is Canon Solutions America helping its customers?

We try to make sure they understand our five-pillar layered approach to security offerings, as well as our commitment to making solutions and services that help protect their businesses available. One of the key pillars is cybersecurity, where we make subject matter experts available for consultations, assessments and in the unfortunate event, incident response to recover from a breach.

What investments are you putting into these initiatives?

We regularly host events with our Print Customer Council, a select group of commercial and in-plant printers, to make sure we're meeting their needs and learn where we can do more. We conduct webinars and provide regular thought leadership content to our greater production audience. Our recent investment in security solutions partners is another step in that direction. File level encryption technology providers, secure content collaboration, mail security and computer-based security training are recent examples. ■