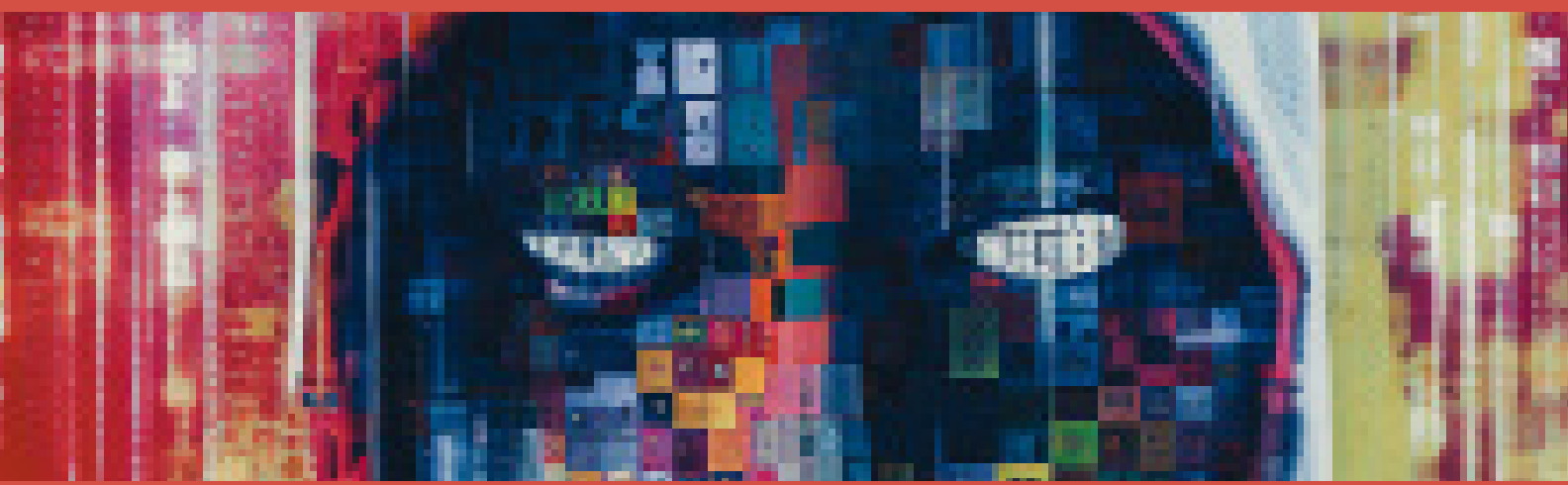
M+E JOURNAL

A SECURE AI WORLD?



How AI is being used both by and against the industry

SECURITY SOLUTIONS
Where and how AI is being used to attack and protect M&E

SMART CONTENT
Massive amounts of data now required new tools, including AI

23.02

PROTECTING THE CONTENT SUPPLY CHAIN

By following best practices, any organization can be prepared to fend against cyberattacks

ABSTRACT: Every day, the world depends on the supply chain of products and services for everyday tasks. How can organizations ensure that content shared with third parties stays safe? What is the impact of having a weak cybersecurity posture in your content supply chain, and how can these risks be mitigated? This article will examine the risks inherent in the content supply chain and identify best practices to defend your supply chain against potential risks.

By Chris Williams, Senior Cybersecurity Consultant, Richey May Cyber

The content supply chain involves creating, managing, and distributing digital content across various platforms and channels. Content can include documents, images, videos, audio, software, data, and more. Third parties, such as suppliers, customers, partners, or contractors, interact with this content for various purposes, such as collaboration, marketing, or outsourcing.

However, sharing content with third parties exposes it to potential threats such as theft, tampering, corruption, or unauthorized access. These threats can compromise the confidentiality, integrity, and avail-

BY FOLLOWING THESE BEST PRACTICES, you can protect your content supply chain from cybersecurity risks and ensure that your content stays safe and secure throughout its lifecycle.

ability of the content, as well as the reputation and trust of the organization. Moreover, these threats can have severe consequences for organizations that must comply with GDPR, PCI DSS regulations, and others.

Therefore, organizations need to protect their content supply chain from cybersecurity risks. Some of the best practices to do so are:

Conduct a risk assessment of your content supply chain. This assessment will identify the types of content you share, the third parties you share it with, and the platforms and channels you use to gather a complete understanding of your organization's threat landscape and the potential threats and vulnerabilities you may face. Prioritize the most critical and sensitive content and third parties and implement appropriate security measures accordingly. Review the past internal security risk assessments performed to meet TPN requirements.

Encrypt your content before sharing it with third parties. Encryption transforms data into an unreadable format, usable only after an authorized party uses a key to decrypt it. Encryption protects your content from unauthorized access, modification, or disclosure. You can use encryption tools such as BitLocker, FileVault, VeraCrypt, or others to encrypt your content on your devices or storage media.

Use secure methods of sharing your content with third parties. Avoid using insecure methods such as email attachments, USB drives, or public links that can be easily intercepted or compromised. Instead, use secure methods such as VPNs, secure file transfer protocols (SFTP), or secure cloud services that offer end-to-end encryption and authentication. You can use tools such as Tresorit, MEGA, or others that encrypt data on the client side before uploading to the cloud.

Monitor and review your content supply chain. Keep track of who accesses your content, when they access it, where they access it from, and what they do with it. You can use tools such as Splunk, Arctic Wolf, or others to collect and analyze logs and events from your devices, platforms, and channels.

Respond to alerts from the monitoring systems. When alerts come from the monitoring feeds that are in place, it is crucial to be able to respond quickly. You can use tools that assist in the response process, such as Arctic Wolf, CrowdStrike, or others, to alert you to the actions to take.

Educate and train your employees and third parties on good cybersecurity hygiene. Human error is one of the leading causes of cybersecurity breaches in the content supply chain. Therefore, raising awareness and educating your employees and third parties on handling content securely and responsibly is essential. You can use tools such as Arctic Wolf, KnowBe4, or others to deliver online training courses and simulations on phishing, ransomware, password management, data protection, and more.

Review all the steps above regularly to ensure that security gaps are remediated in alignment with evolving cybersecurity threats.

By following these best practices, you can protect your content supply chain from cybersecurity risks and ensure that your content stays safe and secure throughout its lifecycle. Questions about how to secure your content supply chain? Contact info@richeymay.com to learn more about strengthening your content's defense shields. ⊞

Chris Williams *is the senior cybersecurity consultant for Richey May Cyber. He has more than 14 years of IT and cybersecurity experience. In his role at Richey May, he works with organizations to bring a better understanding of their security and helps align security with business objectives. Williams has provided assessments and advisory services for clients in the financial, media and entertainment, manufacturing, professional and business services, healthcare, educational, retail, and energy sectors. cwilliams@richeymay.com @RicheyMay*