Top 5 Information Governance Challenges: Threat Awareness

"Fifty-seven percent of respondents are focusing on education and training while fifty-four percent are sharing the vision and benefits of change with their employees." [1]
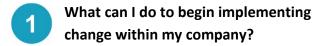
Are employees downloading malware?

When employees download files from LinkedIn, Facebook, YouTube and others, they risk the possibility of downloading malware and other viruses. It is imperative that they keep their anti-virus/malware protection software up-to-date. Information Governance (IG) policies should stipulate the need to monitor how these platforms are used and educate department heads on what the company considers to be best practices.

Change is one of the biggest challenges for most businesses. One of the best ways to address it is through education and awareness. Here are a few things you need to ask in relation to your remediation practices.

- What can I do to begin implementing change within my company?

- How can I stress the impact malware can have on our business?

- What can I do to support my employees when they have questions about potential threats?

> The most effective approach to threat awareness is one that is proactive and forward thinking rather than reactive and short sighted.

1   What can I do to begin implementing change within my company?

Communicate a strategy focused on compliance, ECM and your IG framework as they relate to threat awareness.

2   How can I stress the impact malware can have on our business?

Demonstrate using examples of how malware, and other threats could impact the corporate information ecosystem.

3   What can I do to support my employees when they have questions about potential threats?

Provide contact information and online resources like FAQs for guidance.

Closing Thoughts

Threat awareness is an area where communication can play a key role in bringing about change in the ways people think and act when it comes to using social media tools and randomly opening email attachments. Most instances of malware infection are not due to the employee maliciously causing it but rather unwillingly causing it to happen.

There are many resources available to help if you do not have the expertise available in-house. There are consultants, contractors, and even closer than you may think, your solutions providers. These are folks who work with their customers every day to ensure their business needs and requirements are met, and have been involved in many operations worldwide. Seek their advice as well. You can also download the latest eBook on this topic titled "Minimize Business Risk – Top 5 Information Governance Obstacles You Must Tackle Now" to get some great insight on steps you can take today.

Bob Larrivee is Vice President and Chief Analyst of AIIM Market Intelligence.

---

1. **Minimize Business Risk: Top 5 Information Governance Obstacles You Must Tackle Now**

Produced in partnership with:

About Canon

Canon Business Process Services, a wholly owned subsidiary of Canon U.S.A., offers information governance services that address the controls and metrics necessary to capitalize on valuable information and to establish governance across the enterprise. We also provide managed services and technology for information and document management, business process outsourcing and specialty workforce services.

Our mission is to help clients improve operational performance while reducing cost and risk. Canon Business Process Services has been named a Global Outsourcing 100 Leader by IAOP for the past eleven years and recognized in the Gartner Magic Quadrant for Managed Print and Content Services for five consecutive years. We have also been acknowledged by CIOReview magazine as a "20 Most Promising Legal Technology Solution Provider."

Learn more at cbps.canon.com and follow us on Twitter @CanonBPO.