16 things you should be doing to secure print and documents

KOFAX

Shahid Shah
CTO,
Citus Health, Inc.

Dan Lohrmann
Chief Security
Officer, Security
Mentor, Inc.

Scott Schober
Cybersecurity
Expert & Author
of Hacked Again

Stacy Leidwinger
VP of Product –
Imaging, Kofax

Robert Stasio
Managing Director,
Dreamit Ventures

Tyler Carbone
COO,
Terbium Labs

Mark Gross
Senior Principal
Product Manager,
Kofax

KOFAX

Hardware & Software

Processes

Data

People

KOFAX

Understand the exposure

“What is the one solution that everyone in your organization has access to and is accessed by many of your key business systems? It is your printer. Yet when it comes to data security, all too often it is the one area that is overlooked.”

Stacy Leidwinger, VP of Product – Imaging, Kofax

KOFAX

Set higher standards

“Hold printer and fax device manufacturers to the same level of scrutiny as computer servers. Print/fax have the same baseline security vulnerabilities but then they are more vulnerable because there are additional capabilities which other servers don’t have.”

Shahid Shah, CTO at Citus Health, Inc.

KOFAX

Enable all security

“Enable the security features that are available, including stronger Wi-Fi security settings. Follow best practices. Do an assessment of current configurations—know what you have in place now. Change default settings and passwords.”

Dan Lohrmann, Chief Security Officer at Security Mentor, Inc.

Establish a security framework

“Focus on hygiene (updates, best practices, etc.), implement the best defensive technologies you can, and set up within a risk management framework that minimizes damage if a breach occurs and ensures that operations can continue after it does.”

Tyler Carbone, COO at Terbium Labs

Implement 24/7 monitoring

“The best prevention mechanism with connected devices is monitoring. There are multiple vendors in the IoT space which can look at a network tap and monitor threats across all connected devices.”

Robert Stasio, Managing Director at Dreamit Ventures

Hardware & Software

🔒 Processes

Data

People

KOFAX

Create clear policies

“Writing a clear internal policy is essential to print and document security. When printed documents are not removed from the outbound print tray, they need to have a short life before they need to be shredded.”

Scott Schober, Cybersecurity Expert & Author of Hacked Again

Minimize vulnerabilities

“Check workflows associated with the utilization of fax and printing—encourage their use when it makes sense but remove the steps from workflows where security is more important than convenience.”

Shahid Shah, CTO at Citus Health, Inc.

KOFAX

Use tools that reduce risk

“Obtaining signatures can add layers of documents as you need to print, scan, and email. These stages allow sensitive data to be at risk of being copied or intercepted. Utilize tools such as DocuSign to maintain security and minimize all the extra printing.”

Scott Schober, Cybersecurity Expert & Author of Hacked Again

Automate processes

“The best process is one that is automated. The more processes you can automate, the less security risk you will face and you will have an auto-generated audit trail for internal and external audits.”

Stacy Leidwinger, VP of Product – Imaging, Kofax

KOFAX

Hardware & Software

Processes

Data

People

KOFAX

Audit your data

"Start implementing auditing of storage on print/fax servers to see what data is being left on those devices that could potentially be exploited."

Shahid Shah, CTO at Citus Health, Inc.

Go digital

“A significant amount of print is created simply to access a single piece of information within a larger dataset, after which the entire printout is discarded. Converting back-office print to electronic delivery gives the user access to the information without the risk of ink on paper or the waste of resources.”

Mark Gross, Senior Principal Product Manager, Kofax

Add intelligence

“By adding intelligence and rules you can ensure that private information is never even inked on the page. Data security starts with ensuring that only the information allowed to be printed for viewing is printed.”

Stacy Leidwinger, VP of Product – Imaging, Kofax

KOFAX

Hardware & Software

Processes

Data

People

KOFAX

Train and raise awareness

“Microsoft Excel and Microsoft Word are two of the most commonly used business programs, yet many users do not utilize the password protection feature to restrict unauthorized users from opening and/or modifying the document.”

Scott Schober, Cybersecurity Expert & Author of Hacked Again

KOFAX

Respect user experiences

“Convenience drives compliance. When enforcing print security measures, you need to make it seamless for your workers so they will not look for ways to bypass the security you have in place.”

Stacy Leidwinger, VP of Product – Imaging, Kofax

Actively review activity

“Companies implement print and scan management software which capture audit logs and reports of user activity, but then fail to review the logs for suspicious activity (e.g. significant printing after-hours). Regular reviews can identify security issues earlier.”

Mark Gross, Senior Principal Product Manager, Kofax

KOFAX

On and offboard access

“A critical step many companies overlook is to ensure when an employee leaves, retires, or is terminated, their access to the network is revoked so they cannot download any sensitive documents.”

Scott Schober, Cybersecurity Expert & Author of Hacked Again

Ensure print and document security

1. Understand the exposure
2. Set higher standards
3. Enable all security
4. Establish a security framework
5. Implement 24/7 monitoring
6. Create clear policies
7. Minimize vulnerabilities
8. Use tools that reduce risk
9. Automate processes
10. Audit your data
11. Go digital
12. Add intelligence
13. Train and raise awareness
14. Respect user experiences
15. Actively review activity
16. On and offboard access

KOFAX

Learn more about your print security risks at www.kofax.com/DocumentsAreDangerous

KOFAX