CIO FROM IDG SPONSORED CONTENT

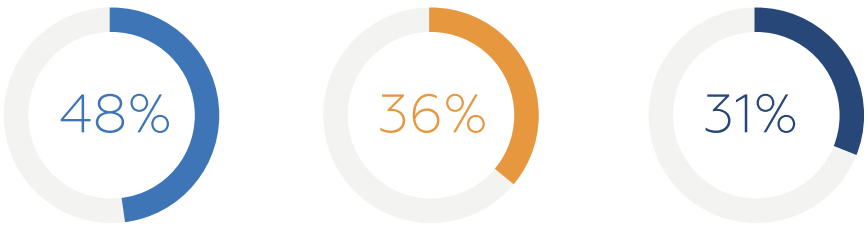
WHITE PAPER

SECURE IT ASSET DISPOSITION IS CRUCIAL FOR PREVENTING DATA BREACHES, PRESERVING REPUTATION

Companies that fail to keep track and properly dispose of their IT assets face a number of significant risks, including data breaches, fines, and potential damage to their company's reputation.

But a secure IT asset disposition program can help to reduce the possibility of a data breach. In a recent webcast presented by IDG and Iron Mountain—*Preventing Data Breaches Through Secure IT Asset Disposition*—Bob Johnson, CEO of i-Sigma, and Brooks Hoffman, Principal of Secure IT Asset Disposition at Iron Mountain, discussed misconceptions about IT asset disposition, real-life business cases, the changing landscape of IT asset disposition, and how to position your organization in order to mitigate these types of data security risks.

TOP CONCERNS IN ITAD



SOURCE: IDG & Iron Mountain Research 2019

IRON MOUNTAIN®

3 Reasons why ITAD is Important: (1) Regulation (2) Avoid damaging headlines (3) Protect Intellectual Property

As CEO of i-SIGMA, the nonprofit trade association representing more than 1,700 data security and information management member locations around the world, Johnson has over 40 years of experience in data protection and regulatory compliance—and has seen many scenarios firsthand.

First and foremost, organizations across the globe must prioritize IT asset disposition to ensure compliance with a variety of data protection regulation requirements. "Legally, you have to protect the personal information of your employees and the clients that you work with," Johnson said.

In the US, companies are subject to both state and federal laws to protect residents' personal data. Experts also believe that federal data privacy legislation in the US isn't far off, while in the European Union, the General Data Protection Regulation of 2016 allows people to obtain data that companies have collected on them and have their records deleted. Regulations are and will always be changing, making it critical for organizations to have a sound plan in place.

Another reason to prioritize IT asset disposition: failing to protect employee and client data can result in expensive and brand-damaging headlines.

For example, in the last year, a large international investment bank, unaware of how they had disposed of their IT assets four years prior, had to notify hundreds of thousands of clients that their information had been put at risk.

"They had to do the breach notification simply because there was the potential that [assets] had been put at risk," Johnson said—and they were fined $60 million. "Breach notifications are very expensive."

In the case of missing IT assets, Johnson said that every one of the assets "is a potential time bomb. There is no statute of limitations on breach notification. IT asset disposition is not something that can be ignored. In fact, I would go so far as to say if it is ignored, it will be a problem."

A third reason to strategically focus on secure IT asset disposition is to protect intellectual property, both Hoffman and Johnson said. Companies that concentrate solely on the personal information they're required to by law to protect may miss out on the fact that improper disposal puts their intellectual property protections at risk.

If companies can't establish that they were protecting proprietary information, such as a trade secret, for example, they may no longer have the rights to that information. "They literally can lose their right to protect it," Johnson said. "They have to show they've been demonstrating that security throughout."

Where your program needs to focus

While some companies are cognizant of these threats, today many are prioritizing methods of data destruction when they should instead be creating a comprehensive, secure IT asset disposition framework that includes sound policies.

"Sometimes organizations focus on the trees as opposed to the overall forest," said Hoffman. "They mistakenly focus on methods of data destruction and individual specifications, as opposed to creating an overall framework for their IT asset disposition program—including and encompassing a well-documented set of policies and procedures."

"IT ASSET DISPOSITION IS NOT SOMETHING THAT CAN BE IGNORED."
BOB JOHNSON, CEO OF I-SIGMA

Companies may overly fixate on destruction methods, such as wiping via software, either onsite or offsite; shredding certain types of media; or degaussing, which involves subjecting magnetic media to a very high magnetic field to purge it. Some organizations also create detailed policies about shred size, and assume, when it comes to the ability to prevent recovery of data off the media, the smaller, the better.

"This really misses the point," Hoffman said. Instead, leaders must be able to track the status of their data-bearing assets through their entire life cycle. "That means from procurement, during their in-service life, and then through final disposition."

It's this so-called "cradle to grave" approach that's so critical when creating an IT asset disposition program, both Hoffman and Johnson said.

What's the solution?

Senior executives may not be directly involved in IT asset disposition decisions, but there's still plenty that they can do to understand and reduce the risks associated with it by helping to create this important "cradle to grave" approach and a sound IT asset disposition program. Proper IT asset disposition should be viewed as a data security and environmental sustainability investment versus a waste disposal cost.

1 Identify the Sensitive Data

Focus on systems and work to both understand which company assets contain sensitive data and where these key assets are located. For example, data-bearing assets are traditionally thought of as laptops, PCs, and servers, while there is other crucial equipment in play as well.

"There's data resident in many other devices that don't traditionally come to mind," Hoffman said, including medical testing equipment or even copy machines. "You really have to have good systems in place in order to understand where the assets are, where they're located, and what sensitive data is resident on them."

2 Establish Consistent Policies & Procedures

IT and business leaders can also work to ensure that consistent policies and procedures are implemented across their organization and they can commit to monitoring compliance. Organizations may have a well-documented binder full of policies and procedures, but all employees need to be aware of them and follow them—especially in larger, more distributed organizations. Training staff is key.

"It's important that everyone in your organization understands what your policies and procedures are," Hoffman said. Then, consequences must exist for noncompliance, as well as a way to monitor whether employees are indeed complying. "Because again, if there are no consequences, people generally won't follow the procedure steps, and you'll have a very patchwork quilt and decentralized system."

3 Focus on Secure Chain of Custody

Focus on secure chain of custody and the nature of the data rather than a one-size-fits-all approach to processes and data sanitization methods.

In other words, leaders should assess whether data are sensitive or routine. Classified data could be destroyed onsite to avoid breaches during transit. Routine, less sensitive data like schedules or addresses can be sanitized offsite as long as there's a secure chain of custody between the premises and the ultimate processing location.

4 Be Diligent in Vendor Selection

Finally, to avoid bad actors, leaders should ensure that their organization is diligent in vendor selection and look for strategic partners, rather just a vendor. Look for partners who comply with all regulations and industry best practices, choosing credible partners when disposing of assets.

Third-party partners with trusted certifications specific to data destruction, such as i-Sigma's, are an important first step. Other examples of relevant certifications include the e-Stewards and R2 standards, which apply to IT asset disposition. Leaders should also commit to doing their own due diligence while selecting a vendor.

"It's not enough just to look for the certification," Hoffman said. "We read stories from time to time of shady companies that have shipped e-waste overseas, or they've been landfilled, and that may result in data breaches and environmental violations. Again, it's important to choose very credible partners when you're disposing of these assets. You've got to kick the tires yourself."

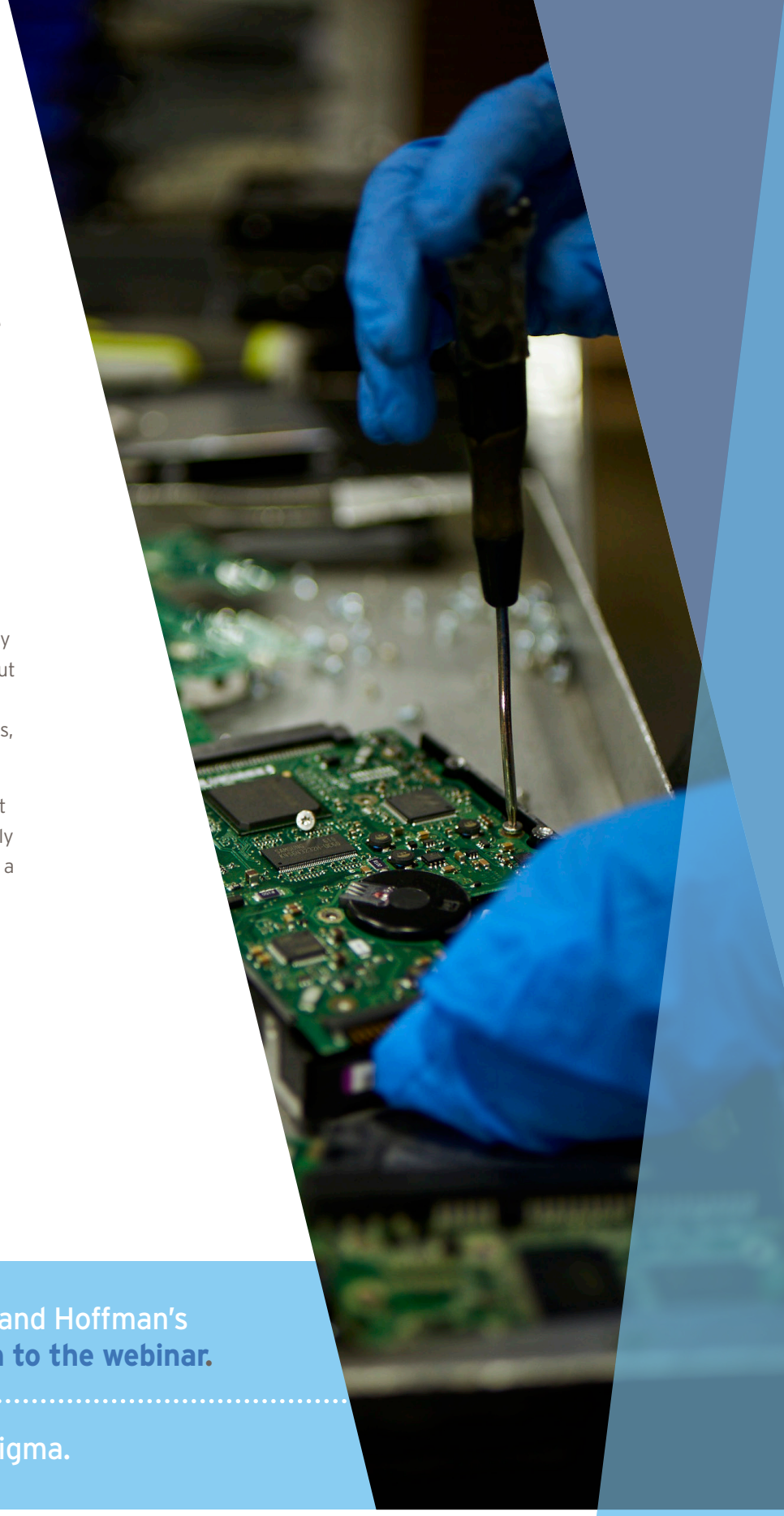
Due diligence can include visiting potential partners' facilities, reviewing their policies and procedures, and checking customer references.

The bottom line

Overall, leaders play an integral role in shaping a comprehensive and secure IT asset disposition strategy for their organization. By investing in a well-thought-out and designed program, they can help safeguard their companies and protect them from costly data breaches, fines, and potential reputation damage.

"Understanding the nature of the data, how sensitive it is, where it's located, and following through consistently with your policies and procedures are really the key to a successful program," Hoffman said.

In today's environment, added Johnson, if secure IT asset disposition is not addressed, it will ultimately be an issue. "It's just a matter of time."



For more of Johnson and Hoffman's expert insights, **listen to the webinar.**

Click here for information on i-Sigma.