REVERSE LOGISTICS magazine®

Serving Manufacturers, Retailers, and Service Solutions Providers

To view the complete PDF of edition 113
with free registration/log-in
please visit [Editions (rla.org)]

How To Avoid Making Headlines For The Wrong Reasons

By Patty McKenzie, Director of Education and Outreach, SERI – RLA Alliance Member

DATA BREACH
NEWS
BREAKING
NEWS
ANOTHER DATA BREACH CONFIRMED
Compromised information has global implications

Each year a growing number of established and well-known companies find themselves in the headlines for embarrassing – and costly – failures to protect data. Many of these cases can be attributed to the actions of third-party service providers and the failure of organizations to adequately assess the risks when looking for partners to manage returns, trade-ins, and IT Asset disposition. Similar risks are inherent in auctioning used electronics to the highest bidder without doing the proper due diligence on the buyer.

A study on Third-Party Data Risk conducted by Ponemon Institute, a leading research organization dedicated to data privacy and protection, surveyed more than 1000 CIOs and security professionals. Almost 60% of respondents experienced a data breach caused by a third-party service provider – with forty-two percent reporting such a breach had occurred in the previous 12 months. One reason that so many organizations do not have adequate safeguards in place is simply "out of sight, out of mind."

FALLOUT FROM THIRD-PARTY DATA BREACHES

Data security may be front and center for organizations as long as data-containing devices remain in their possession, but many organizations falsely assume their responsibility ends when the devices are sold or transferred to a third-party. However, many regulations involving data privacy hold organizations responsible for the actions of their third-party vendors – and with good reason. Several studies in the past two years analyzed electronics that were being marketed for reuse and found many of those devices contained residual data including social security numbers, passwords, corporate emails and projections, and other sensitive and proprietary information. Particularly alarming was that in most cases it was clear an ineffective attempt had been made to remove the data – which means the third-party responsible for data destruction and remarketing was either unskilled, had cut corners…or both!

Organizations that fail to adequately assess the risks of third-party vendors and exercise adequate due diligence in the selection and management process, are subject to significant fines. Last year, the U.S. Treasury Department levied a $60 million fine to one of the largest international investment banks for failing to exercise proper oversight in its management of decommissioned electronic equipment and the data it contained.

COURT OF PUBLIC OPINION

Separate studies conducted by Cone Communications and by James Rubin and Barie Carmichael (Published by Columbia Business School) find that consumers have extremely high expectations when it comes to corporate responsibility – and that how well companies measure up in meeting those expectations has tremendous impact on consumer loyalty and purchasing decisions.

HOW TO MINIMIZE YOUR RISK

Virtually all third-party vendors, buyers, or remarketers will claim to be a responsible vendor, but unfortunately, that is not always the case. Any vendor can print a “Certificate of Destruction,” but do the actions of the vendor match the words on the paper? When selecting partners to manage electronic returns, trade-ins, remarketing or disposition, thorough due diligence is essential for reducing risk in the reverse supply chain.

This includes verifying things such as:

- Chain of custody – Who will have access to products? Various types of electronics are often processed by a network of different vendors who specialize in specific types of processes. Do you know all the vendors handling your electronic equipment? And do you know the final destination of that equipment?
- Does your vendor disclose how your data will be sanitized, and whether it will be done internally or by another vendor?
- Is the vendor or reseller qualified to effectively sanitize residual data?
- What quality control and security measures are in place?
- Does your vendor provide detailed records of successful data erasure by device?
- What happens to the devices that fail to be sanitized? Are you provided evidence of physical destruction?
- Does the vendor or reseller comply with applicable legal requirements for data, environment, health and safety?
- What evidence does the vendor or reseller provide to demonstrate conformance to best practices and legal requirements?

If you do not know the answers to these questions, your organization could be at risk. The new R2v3 Standard (free to download) provides a great roadmap for evaluating your vendors. Core Section 7 outlines data security controls that every vendor involved in the handling or processing of your electronic equipment should be implementing. And additional measures and controls should be in place for vendors that perform the actual data sanitization. The requirements in Appendix B of the R2v3 Standard serve as a good benchmark to follow. The combination of Core 7 and Appendix B can provide a good guide for performing your own due diligence.

Self-made claims by vendors are not always reliable. Simply asking your vendor to fill out a questionnaire to self-report their compliance with these best practices, does not provide adequate assurance that data-containing devices will be securely managed and data effectively sanitized. Without verification, there can be little confidence in the vendor's response. But verification can be challenging because data security is a complex topic and hard to evaluate.

THIRD-PARTY CERTIFICATION CAN BE AN EFFECTIVE DUE DILIGENCE TOOL

Another way to verify that your vendors have implemented the best practices in Core 7 and Appendix B is to use the third-party certification model. Every facility certified to the R2v3 Standard is evaluated each year for conformance to the Core 7 data security requirements -- and every facility certified to Appendix B has met the additional requirements that apply specifically to data sanitization.

R2 addresses the full reverse supply chain, from first use through end-of-life. The latest version of the Standard, R2v3, has further raised the bar for data security as well as for practices that maximize responsible reuse and support a circular economy for electronics. And comprehensive annual audits of R2 Certified facilities provide oversight and accountability for increased confidence in R2 Certified vendors.

With nearly 950 R2 Certified facilities operating in 33 countries, partnering with R2 vendors can be a powerful way to help your organization avoid making headlines for the wrong reasons. You can search for an R2 Certified vendor at https://R2directory.org.

To learn more about R2 requirements and how R2 Certified Partners reduce risk in the reverse supply chain, visit the R2 website: https://seriR2.org

AUTHOR

Patty McKenzie is Director of Education and Outreach for SERI, a nonprofit organization that champions electronics sustainability. SERI is most well-known for its development and oversight of the R2 Standard and Certification Program – a program that requires responsible reuse and disposition of electronics throughout all stages of the product lifecycle.