WSJ PRO
CYBERSECURITY

EU Rule Prompts Security-Focused Tech Recycling at U.S. Companies

An Electronic Recyclers International shredder moves hardware along on a conveyor belt, then slices and crushes it.
PHOTO: ERIDIRECT.COM

By Catherine Stupp
May 6, 2019

GDPR has sparked a rush to safely dispose of old technology among companies worried about exposing sensitive data when getting rid of computers and devices, resulting in a boom for specialized recyclers.

To comply with the European Union's General Data Protection Regulation, U.S. corporations are seeking out specialized data-destruction and sanitization services to ensure their hardware is stripped of any personal data, according to recycling businesses. Under the law, companies that do business in Europe, or collect data from people there, are liable for exposing information that can identify an individual.

The stakes are high: GDPR violations can bring on fines of up to 4% of global revenue or €20 million ($22 million), whichever is larger.

“The velocity is like nothing we’ve seen before,” said John Shegerian, executive chairman of **Electronic Recyclers International Inc.**, a Fresno, Calif.-based company that shreds discarded devices around the country.

Cybersecurity professionals are now often part of initial discussions when they approach **Executive Personal Computers Inc.,** a recycling company in St. Charles, Mo., specializing in hardware destruction, Chief Technology Officer Brian Wahoff said. In the past, asset managers and financial officers usually handled recycling contracts, Mr. Wahoff said.

Around 40% of devices for sale on second-hand marketplaces and advertised as having been wiped of personal data still contained sensitive information, according to a 2017 **National Association of Information Destruction** study of 250 used devices. Half of the tablet computers examined contained information including credit-card details, names, addresses, photos, usernames and passwords.

Some companies ask ERI to destroy hardware at their offices if data is too sensitive to travel, Mr. Shegerian said. ERI trucks bring in mobile shredders that slice and crush the equipment. Customers’ security or IT teams can observe the destruction first-hand.

None of the destroyed materials are sent to landfills, Mr. Shegerian said. Batteries and ink cartridges are removed and recycled, while processed plastics are sold to firms that reuse them.

Corporate cybersecurity and legal teams often focus on GDPR measures that require them to identify and disclose what personal data they collect. Disposing of devices can be an afterthought, said Daniel Fabiano, a partner in the Toronto office at Canadian law firm **Fasken Martineau DuMoulin LLP**.

“It’s just as important to ensure that you’ve securely destroyed the data as it is to ensure that you’re allowed to hold the data in the first place,” he said. Companies shouldn’t leave tech disposal to third-party vendors without vetting their policies for GDPR compliance, he advised.

EPC's Mr. Wahoff said GDPR, which went into effect last May, brought a surge of business last summer.

EPC charges on average $8 to $10 to erase data from a single device and $8 to $9 to shred a piece of hardware, though prices vary, Mr. Wahoff said.

Mr. Shegerian said ERI’s prices depend on the type of material and whether it's done on or off site. “It’s not cheap,” he added.

Over the past two decades, regulation has prompted steady growth in the number of U.S. businesses using data-destruction services, said Robert Johnson, chief executive of the National Association for Information Destruction.

“It’s become a customer-relations issue and a regulatory issue. It’s gone from the basement to the boardroom,” Mr. Johnson said.

Still, many companies neglect data-security problems on devices they dispose of or reuse, said Jordan Rae Kelly, senior managing director at FTI Consulting.

“Their only concern is when your device is in front of you and how well it’s operating. When it’s over, people think the security risk is over,” she said.