TECH & CYBER

CUSTOM CONTENT • February 17, 2020

A Culture of Privacy Includes Proper Handling of Recycled Computers

By Genevieve Walser-Jolly, Scott Hyman, and Gary Scott

In December, Severson wrote “What Does a Data Privacy Program Look Like?” In that article, we discussed how to design a privacy program that includes all aspects of a business. We now want to highlight one, often overlooked, component of a data privacy program – disposing of information on recycled computer equipment.

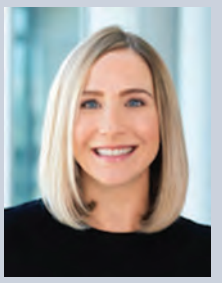
Many businesses don’t realize they have specific data destruction obligations when it comes to disposing of or recycling their computer equipment. Many federal data privacy laws (HIPAA/HITECH, GLBA, IRS Media Sanitization Guidelines, and FACTA) contain a data disposal component. Each includes something similar to the Federal Trade Commission’s Disposal Rule (FTC):

“According to the FTC, the standard for the proper disposal of information derived from a consumer report is flexible, and allows the organizations and individuals covered by the Rule to determine what measures are reasonable based on the sensitivity of the information, the costs and benefits of different disposal methods, and changes in technology.”

It is helpful to know that the FTC and other privacy laws expect businesses to take precautions but unfortunately, businesses are left to decide what “reasonable” means for their business. We know from case law in California, that having no security procedures and practices in place is unreasonable. This includes a plan to securely destroy data when retiring computers.

The California Consumer Privacy Act (CCPA) was passed in 2018 and provides a private right of action for data breaches. A business who fails to properly destroy data on its recycled electronic devices and subsequently experiences a related data breach, can face statutory damages of $100 to $750 per person. Whether a business had “reasonable” security procedures and practices in place is a defense to such a class action.

Simply deleting or reformatting hardware is not enough. Finding a vetted company that meets stringent standards and documenting the engagement of such a company is key. Taking basic precautions can save a business from civil liability and help a business defend against regulatory enforcement actions down the line.



Genevieve Walser-Jolly (CIPP/US) is a partner and Scott Hyman (CIPP/US, CIPP/E, CIPP/M) is a shareholder at Severson & Werson, APC. They help clients setup data privacy programs, turn-key data breach responses, and CCPA compliance. They can be reached at grw@severson.com and sjh@severson.com.

Gary Scott is the President of E-Waste Security. E-Waste Security provides digital media destruction services. They specialize in NIST 800-88 compliant data destruction. He can be reached at gary@ewastesecurity.com.

Your Company Was Hacked. *Now What?*

Dealing with cyberthreats is part of doing business for organizations of all sizes and specialties. According to the FBI, the costs of dealing with cybercrime doubled to $2.7 billion between 2017 and 2018. And recently, CNBC reported that the average cyberattack now costs $200,000, with 43 percent of cyberattack victims being small businesses that may be hard-pressed to take a hit of that magnitude.

One small slip-up by a busy employee or executive can leave your business wide open for cyberattack. An August 2019 story in The New York Times cited the experience of a city employee of Allentown, Pennsylvania, who was using a laptop while on a routine business trip. While traveling, he happened to miss a software update.

After he clicked on a "phishing" email sent by Ukraine-based hackers, he unwittingly allowed malware to spread on computers throughout his office. It cost the city more than $1 million to clean up the damage.

Even digital giant Facebook has not been immune from attack. In 2018, it disclosed that a data breach had allowed illicit access to 30 million accounts. Selling people's data is a lucrative prospect, so it's clear that cybercrime is not going away.

Other corporations, municipalities and hospital systems have been paralyzed by ransomware attacks. It's a more common threat than you might think. In these attacks, hackers target a corporation's digital systems to paralyze functions such as records, email and other services. Then they hold the corporation hostage, saying they won't free up the software unless they're paid off.

Some other common types of cyberattacks are:
• *Stolen passwords.* Phishing emails trick people into going to websites where they're asked to enter their usernames and passwords. The sites look authentic enough – but they're fake, and give hackers access to a wealth of company and/or personal information.
• *Social engineering.* Similarly, a phishing email is sent to employees and it looks like it comes from someone within the organization. It will ask for sensitive information such as passwords.
• *Phony hyperlinks and attachments.* Again, they may look legitimate. But when someone clicks on the link or opens the attachment, they give hackers an inroad to their computer system.
• *Spamming.* Spam emails might look like helpful ads for beauty products or cheery promises of free stuff. But they can trick people into providing personal information, which can be sold on the black market.
• *Hacked versions of software.* Fake versions of legitimate software (such as an online meeting program) let cybercriminals lift data or lock down office computers.
• *Malicious mobile apps and downloads.* Mobile devices can pose risks, with so many people doing business on their smartphones. An employee who OKs permissions for a malicious app can give hackers access to sensitive company data.

About the Author
Kevin Studley is the president of The Network Pro, Inc. a California based Managed IT and Security company that that specializes in information security based on the NIST framework. The Network Pro is recognized as a growth company on the Inc. 5000 fastest growing companies list, a Great Place to Work by the OCBJ, and has placed on the Top 501 Managed Services Providers list for the last seven years. Kevin Studley is an active and long-standing member of Vistage and actively participates in events that promote the business community. For more information, visit www.thenetworkpro.net or call (714) 333-9620.