

SECURING THE FUTURE

In this Issue

- We're not digital yet
- How Millennials affect the workplace and data security
- Data breach roundup
- Customer connections



We're Not
Digital Yet

In today's business environment, the majority of organizations are not paper free; the average office worker still uses 10,000 sheets of copy paper every year, which translates into 4 million tons of paper across the U.S.¹ Since paper remains a core component of office life, there are still plenty of hard drives, printers, fax machines, photocopiers and other similar devices in every office.

Unfortunately organizations don't often realize that these devices are storing confidential information on hard drives and as a result may not be taking proper precautions in disposing of their devices. According to the 2014 Shred-it Security Tracker, 39 percent of US businesses surveyed have never disposed of hard drives, USBs or other hardware that contain confidential information which translates into a large amount of confidential data that could potentially fall into the wrong hands.²

Once a hard drive is unused, the only way to ensure that the data on it is completely gone is to remove the hard drive from its device and securely destroy the hard drive before throwing it away, recycling or selling it.

800.697.4733 | shredit.com



Making sure
it's secure.™

SECURING THE FUTURE

Three Simple Workplace Guidelines Designed to Safeguard Hard Drives:

1. Perform a regular cleaning of storage facilities and avoid stockpiling unused hard drives.
2. Destroy all unused hard drives using a third-party provider who has a secure chain of custody and confirms destruction, to help give you peace of mind and ensure your data is being kept out of the hands of fraudsters.
3. Regularly review your organization's information security policy to incorporate new and emerging forms of electronic media.



800.697.4733 | shredit.com

How Millennials Affect the Workplace and Data Security

Millennials, those born in the 1980's and 90's, are quickly becoming one of the most influential and dominant employee sectors in the workplace. By 2020, nearly 50 percent of the U.S. workforce will consist of Millennials, according to the U.S. Bureau of Labor Statistics.³

With significantly different values than their predecessors, this generation leans towards technology and flexibility creating a need for organizations to adapt policies and procedures. In terms of data protection, this involves ensuring policies meet the growing dependence on technology while still retaining the security of confidential information.

Despite being driven by technology, Millennials appear to have a lack of regard of data security and the protection of their personal identifiable information.⁴ From an organizational standpoint, this lack of concern surrounding online security needs to be addressed and mitigated through company-wide policies related to smartphone apps and [for personal devices](#) used in a work capacity.

Nearly 70 percent of Millennials continue to use personal apps in the workplace to support their work.⁵ Of that population, 60 percent don't express concern about corporate security when using these personal apps. When you consider that 25 percent of employed U.S. adults have been a victim of hacking on a personal device, it should be a significant concern of employers that these devices are not only in the workplace but are not used under strict security guidelines.⁶

For tips on building a BYOD policy or how to keep confidential information safe, please visit the Shred-it Resource Center at shredit.com/resource-center.



Making sure
it's secure.™

SECURING THE FUTURE

Data Breach Roundup

The first step in fixing a problem is knowing that it exists. In each edition we feature a high profile data breach to show businesses how they can mitigate similar risks.

This quarter we wanted to feature interesting research on data breaches in the medical industry.

Journal of the American Medical Association:

A recent research letter published in the Journal of the American Medical Association showed that between 2010 and 2013 there were 949 data breaches exposing more than 29 million health records throughout the US.⁷ Among those breaches, 58 percent were the result of theft, with 11 percent resulting from improper use or disposal.

Just as interesting is the finding that 38 percent of the breaches came from a portable electronic device or laptop, and 22 percent of the breaches were paper documents.

What you can do: It's clear that the medical industry needs to improve security around confidential medical records, and there are simple steps a company can take to reduce the risk of a data breach.

1. Provide clear protocols for the disposal of information that is no longer needed including unused electronic storage devices.
2. Ensure employees remove portable devices from the office only when necessary.
3. Don't allow people to keep unsecured documents on their desk, and be sure to implement a shred all policy for unused documents.



800.697.4733 | shredit.com



Making sure
it's secure.™

SECURING THE FUTURE

Customer Connections

Shred-it's most important relationship is with its customers, which is why Shred-it Partners are trained to provide top level customer service and expertise. In each edition we highlight a Shred-it Partner that went above and beyond to provide exceptional customer service.

Walter Carter

Customer Security Representative, Washington, D.C, Shred-it

Walter Carter goes above and beyond to ensure he meets his customers' needs. He highly values their trust and always focuses on the way he conducts himself to ensure he does not let them down.

"The fact that people trust in me to ensure their confidential materials are safe and secure means a lot to me. My main goal is to make my customers happy and instill a level of confidence so that they know I won't let them down."

Walter credits Shred-it and the company's dedication to customer service with making his job easier. His favorite part of the job is the chance to meet and learn about new people he would never have otherwise met.

Shred-it would like to commend Walter for his integrity and dedication to exceptional customer service work.

For more tips on improving information security, please visit the Shred-it Resource Center at shredit.com/resource-center

You can also stay informed with Shred-it on [Facebook](#) and [LinkedIn](#) or you can follow us on [Twitter](#) at @Shredit

1. Mashable, 2014, *Average U.S. Office Worker Uses 10,000 Sheets of Paper Per Year*
2. Ipsos Reid, 2014 Security Tracker, *American Businesses Deprioritizing Information Security*
3. Financial Post, 2013, *Like it or Not, Millennials Will Change the Workplace*
4. DarkReading.com, 2015, *Will Millennials Be the Death of Data Security*
5. Adweek, 2014, *Why Millennials Ignore Security Protocols at Work*
6. Welivesecurity.com, 2012, *BYOD Infographic: For Security, It's Not a Pretty Picture*
7. The Journal of the American Medical Association, 2015, *Data Breaches of Protected Health Information in the United States*

"I am especially thankful for the driver you blessed us with that day, Walter Carter, CSR."

800.697.4733 | shredit.com



Making sure
it's secure.™