CCS Technologies

October 2018
Volume 13, Issue 10

"Local Support • Personal Service • Since 1976" www.ccstech.net "Relax...we're on IT"

Compliance: To Be or Not To Be…there is no question.

by Jeff Verry

I remember taking Tae Kwon Do in college (not well, if you are looking for someone to defend your business physically, I am not your guy). The instructor was telling us in broken English not to attempt to block a flying spin kick. Think a Chuck Norris kind of thing. Most of us thought, and one of us asked, "Well how am I supposed to defend myself?"

Nodding his head quickly to the side, the instructor said, "Best defense, no be there."

The same principle that might protect your head in martial arts can protect the brain of your network and its critical contents. Whether sensitive data is stored, transmitted or both, it can include financial information, medical records, or personal identifiable information (PII). Each kind of data carries with it certain assumed responsibilities based on what it is and how it is used. These responsibilities are outlined in various industry-specific practices called compliance standards.

The potential consequences to a breach or non-compliance are serious. According to studies published by the Ponemon Institute, threats to your business included:

Cost of remediation - On average it takes 46 days to resolve a cyber-attack.

Loss of customers - 76% of American adults would move away from companies with a high record of data breaches.

Business disruption - This includes costs associated with business process failures and lost employee productivity.

In some cases, you may face regulatory fines, legal costs, and public relations nightmares.

More seriously you may have to deal with the cost of breached client records. Companies like Dell and IBM estimate that a single lost or stolen PII record can cost up to $221 in lost productivity and additional time and effort by you and your staff to make it right. This becomes simple, and dire, math. Take the number of customers, employees, and vendors your business services and uses…multiply by $221…

Worse yet, there is the potential for direct financial loss. Just like a crook can use your credit information for nefarious purposes, it is becoming increasingly common for the bad guys to do the same to sensitive business information and attack your company.

What should you do?

"The best defense is no be there." The best way to deal with a breach is not to have one. We've seen above that a single credit card in the wrong hands or a list of social security numbers misplaced can lead to serious financial consequences. Take every step to proactively make sure that the data that has been entrusted to you by your customers, employees and suppliers is as safe as it can be. Here are some pragmatic recommendations:

Only store what you need to store. The default position should be "do we need to keep this?" Only store credit card information on your computer if you absolutely need to. If you do, see if you can get by using the last 4 digits. The same goes with social security numbers and tax ID's. Similarly, consider how you send information. NEVER send a credit card, SSN, or password over the Internet via email. Always make sure that any website you use has the https and the lock or key icon next to the website address (this is your browser's way of telling you that the website's server is secured). Note that it does not ensure that the website's operator is trustworthy. There is never an alternative to common sense!

Do your homework. Each industry has its own set of best practices and standards. The kinds of technology you use also make a difference. Whether it is PCI, HIPAA or something more specific to your business, get the requirements you need to pass a compliance test.

Consult a professional. Once you have an idea of what you need to do, reach out to *CCS Technologies* for assistance in getting it done! We have experience walking clients through PCI scans, writing up Acceptable Use policies, advising on HIPAA concerns and walking clients through a variety of scenarios.

We can also help you employ scanners that give you an end-to-end picture of possible security vulnerabilities. Whether it is your network infrastructure, server or your desktops, we can scan files, email archives and test the protocols that are in place to make sure that you become or remain compliant.

Give our office a call and schedule a phone consult on where you are and where you need to be with your compliance.

"Relax...we're on IT"

300 Main Street, Coopersville, MI 49404
616.997.TECH(8324)
Fax 616.997.9317

206 Washington, Grand Haven, MI 49417
616.842.TECH(8324)

3489 Kelly Street, Hudsonville, MI 49426
616.669.TECH(8324)

Contact Information

Information	info@ccstech.net
Tech Support	support@ccstech.net
Sales	sales@ccstech.net
Greg Slater	gslater@ccstech.net
Ellen Slater	eslater@ccstech.net
Drew Rowe	drowe@ccstech.net
Jeff Verry	jverry@ccstech.net
Joe Halstead	jhalstead@ccstech.net
Jorge Arias	jarias@ccstech.net
Karen Strickland	kstrickland@ccstech.net
Mark Kowitz	mkowitz@ccstech.net
Ryan McMillen	rmcmillen@ccstech.net
Nick Dykstra	ndykstra@ccstech.net
Eric Ruzek	eruzek@ccstech.net

CCS Technologies Store Hours

Coopersville Store

Mon-Fri 8 - 5:30

Grand Haven Store

Mon-Thu 9 - 6 & Fri 10 - 6
Sat 10 - 3

Hudsonville Store

Mon-Thu 9 - 6 & Fri 10- 6

Lenovo Flex Core i5 Laptop

~~SALE $1099~~

SALE $999

Intel Core i5 1.6 GHz Quad Core CPU w/HT
8GB DDR4 RAM
256GB Solid State Drive
15.6" Touchscreen Display, 1920x1080 / Full HD
Backlit Keyboard & Touchpad
No Optical Drive
2 USB-3, 1 USB-C, 1 HDMI

Setup and Ready to Use!

Prices good through 10/31/2018

While supplies last