Compliance Corner Webinar:

Five Things to Protect Your Systems from Cyber Threats

July 20, 2017

Q: Does ransomware work if everything is stored in a cloud program such as Dropbox or OneDrive?
A: Yes, ransomware can still affect off-site file stores such as Dropbox, OneDrive, and Google Drive. These services work with a 'cached' copy stored locally on a client level computer. As a ransomware application begins encrypting files, these encryptions can be moved to cloud storage services. However, these services all have some form of revision control and allow the user to recover versions as needed, allowing them to restore unencrypted versions. Given the increase in ransomware attacks and how these change and evolve, it is important to keep 'disconnected' data backups.

Q: What about antivirus for Macs?
A: Historically, Mac users believed that their computers just don't get viruses. However, this is not true Microsoft Windows operating systems are simply more widely used, and so there is a higher pool of targets for the virus programmers.

Today, more hackers are targeted the MacOS, because they are a bigger challenge. Mac specific malware, according to McAfee Labs (2017), rose 744% in 2016.

In the end, any device desktop, laptop, tablet and even cellular phones ***need*** to be running actively updated antivirus software.

Q: This has all been about reaction, good and I appreciate it, but is anybody being proactive about locating the "Bad Guys"?
A: Organizations like Symantec, Kaspersky Labs and others are routinely determining the sources of these bad guys, filtering out their IP addresses, updating their security to reflect these known threats. In addition, law enforcement agencies have had to establish interdepartmental relationships with counterparts in other countries. Organizations in-country, such as the Federal Bureau of Investigations, Computer Crime Labs work closely with Her Majesty's National Crime Agency of Britain, as well as private sector groups such as the Infraguardsmen to identify, protect, and prosecute computer crimes.

Q: Is GoDaddy safe for emails with HIPAA and PHI?
A: GoDaddy does offer HIPAA compliant email services for a monthly fee, per user. This is a good indication that the email services they offer free with domain name registration, or are non-specific HIPAA compliant email service is most likely not compliant. More information can be found here: http://tinyurl.com/ycwltddn

Q: Do you cover verifying the cleaning company employees and that they locate password sheets employees put in their desk?
A: This is a very bad practice and is not HIPAA compliant.

Q: Is Dropbox safe to store HIPAA and PHI files?
A: Dropbox is HIPAA compliant, but it is important to note that Dropbox will need to sign a Business Associate

Agreement (BAA) with your organization, as their storage of the data makes them such to the owners of the files.

Q: How do you know if it's a public network?
A: One of the tell-tale signs is that it did not require a password to connect.

Q: If someone uses Norton, Kasperski, McAfee, do they need to be careful with phishing?
A: A Phishing attack falls under the classification of Social Engineering, a complicated way of saying something or someone trying to convince another to openly reveal private information about themselves or their organization without the use of nefarious software. Antivirus software is simply not designed to prevent such activities. There are organizations such a Sophos who are working to prevent such things, but in the end, asking someone about their birthdate is not a computer virus.

Q: What authorities should be contacted in the event of a ransomware attack?
A: It is important to report a ransomware attack. Here are a few organizations by country:

- In the USA, go to the On Guard Online website.
- In Australia, go to the SCAMwatch website
- In Canada, go to the Anti-Fraud Centre
- In France, go to the Agence Nationale de la sécurité website
- In Germany, go to the Bund.de website
- In India lodge a complaint with the cyber crime cell nearest to you.
- In Ireland, go to the An Garda Síochána website
- In New Zealand, go to the Consumer Affairs website
- In the UK, go to the Action Fraud website