By Clinton Henry

Surefire Steps to Lockdown Your Cyber Security

"Dear Client". That's how the letter usually begins.

The next few sentences are a little trickier; there is really no good way for someone to hear that their data has been stolen.

Unfortunately, getting this letter is becoming an all too common occurrence in business. Businesses lose more than $100 billion a year to cyber-attacks and fraud globally.

While a security breach might be one of the last things on your mind, the most recent Travelers Risk Index report shows that it's a top concern for your clients, customers and contractors – "Personal Privacy Loss and Identity Theft" went from barely ranking on their survey a few years ago to being #2, right behind "Financial Security".

The expectation of cyber security has to be met with the same fervor and drive that you strive to meet all your other clients' expectations.

1. Engage and Educate Your Employees

It's important that you create a culture of security within your organization because security is everyone's responsibility. If you don't have buy-in from all your team members, you're exposing your business to unnecessary risk. The majority of attackers gain access to networks via social engineering and the manipulation of a user within an organization, not via command line "hacking" from a dark, Cheetos-filled basement somewhere, as the movies often portray. Why would someone spend days trying to crack your accountant's password when they can simply call your IT desk pretending to be your accountant and ask him to reset it to something new?

2. Anti-Virus

Having an up to date anti-virus deployed on *all* of your desktops and servers is vital. An unprotected computer is an easy target for a motivated attacker. Don't make it easy on them – pay for anti-virus and make sure it's regularly updated by your IT staff.

3. Password Management

It's important that you and your employees leverage strong, complicated passwords that aren't easy to guess. There are now hacking applications you can plug into a computer that will run through the most common 10,000 passwords used in about four minutes, trying each of them. You'd be surprised how many folks with access to critical data have the password of "password," or if they are feeling clever, "password1" (Did this just guess your password? Go change it!).

4. Secure Your Networks

Without getting too technical, just know that having a firewall between your corporate network and the Internet is very important. If you don't, there is very little stopping someone from freely accessing your data.

5. Secure Your Cloud

No matter what cloud provider or service you use, make sure you do your due diligence on their security practices. If they can't easily and quickly tell you how your data is secured, odds are it isn't. Also, for any accounts used to access your firm's data, make sure you have strong passwords and only access it via a computer you own or trust. If you access your cloud on an infected machine, a hacker could potentially learn your password and use it later on without your knowledge.

6. Protect Your Banking Information

Make sure that all financial data, accounts, and records are kept secure and segregated from the rest of your business' general shared drives. If financial transactions are conducted electronically, ensure they are done over an encrypted connection and that your employees never email account numbers, credit card information, or sensitive financial documents.

7. Backups

One of the most common types of breaches now being seeing are called "ransomware" attacks. Instead of "stealing" data from your organization, these attackers find your critical data and then encrypt it (digitally locking you out of it), making it so only the person with the digital "key" can unlock and access that data. The hackers then offer the victim access to the "key" for a very large fee. If you're hit with one of these attacks you have two options: Pay the fee or restore the locked data from a recent backup. This is why backups are so important. Recently a very large hospital, a police department, and a public school (along with literally thousands of other victims) have been forced to pay tens of thousands of dollars to get their data back.

Making sure your data is backed and stored separately from your main repository can help protect you from attacks such as these.

8. Physical Security

This one is self-explanatory but you'd be surprised how much client data is left lying around the office. Ensure your partners, trusted employees, and finance team lock away any sensitive documents when they aren't working with them.

9. Mobile Devices

While they are a convenience and increase productivity of the staff, mobile devices mean that your clients' sensitive data can potentially walk out your firm's door without you ever knowing it. Make sure that all mobile devices used to access corporate data have passwords (your email server can force this requirement), and if you have employees that use laptops you should look at having the hard drives for those machines encrypted. Most modern operating systems have encryption built in (you just have to enable the feature), and it's foolish not to leverage it. If an employee accidently leaves a laptop on a plane or in the back of a taxi, you'll be guaranteed that all data on it is secure and protected.

Your business, your brand, and your bottom line depend on the trust you develop with your clients. Handling the items listed above will go a long way in protecting all three.

Clinton Henry is one of the world's leading cyber security and identify theft experts. Known for his engaging keynotes and insightful perspective on business and personal cyber security, Clinton has amassed a loyal following of business and IT executives who look to him for guidance on how to protect their corporate profits and reputation from attack or compromise. For more information on hiring Clinton for your next event, please visit www.ClintonHenry.com.