Cyber Security 101

by Matt H. Evans, CPA, CMA, CFM

July 10, 2015

One of the most profound challenges facing every company is Cyber Security. Many of us, including myself, are ignorant about the threat. Some of the largest companies are experiencing massive data breaches. Examples include:

- Target Department Stores - Debit and credit card data stolen impacting 100 million customers
- J. P. Morgan - Customer data compromised affecting 76 million customers
- Home Depot – Reported 50 million customer email addresses stolen

"African IT experts estimate an 80% infection rate on all PC's continent-wide, including government computers. It is the cyber equivalent of a pandemic." – Inside Cyber Warfare by Jeffrey Can

The purpose of this article is to bring you up to speed on the problem and actions you can take for reducing the risk. Granted this is not a sexy topic, but it warrants serious attention from every business owner.

The biggest threats facing your company will be targeted at data that can be monetized. Examples include credit card numbers, bank account numbers, social security numbers, and intellectual property. So how do outsiders get access to this data? It's simple – they ask for access. For example, you get a survey that is well written, asking you to provide some information. In some cases, the hacker will offer an incentive to pull you in. In the case of Sony, the hacker gained access through spear-phishing, a practice of knowing something unique about the target company and sending a legitimate and official sounding email. The email message includes a link to an official looking website, asking the recipient to enter user id and password information.

The dilemma facing many companies is lack of awareness. Let's put this in perspective:

- Over 70% of data breaches are discovered by third parties and not the company. Someone notices a strange email or notice, informing you or asking for more information.
- On average, it takes over 80 days for a company to fully detect a data breach and recent studies show that over 10% of data breaches are not discovered until two years later.
- The average cost of a data breach is well in excess of $ 1 million for most companies.

So why is this happening so much? Part of the reason has to do with the availability of hacking software. There are toolkits that just about anyone can use to launch an attack. Additionally, the anti-virus

software that so many of us rely on is six months or more behind the hacker. Hackers subscribe to all of the anti-virus software, staying one step ahead by altering their signatures to get through.

"Whether we like it or not, hackers will get in – and they do get in, every day. The challenge is, yes, to minimize that. But as we get more sophisticated, it's going to be: How do we operate in an environment if we know they're in our systems?" – Heather Crofford, CFO of enterprise shared services, Northrop Grumman

It is absolutely imperative to make sure your people are trained to identify and report anything unusual. For new hires or contract employees, partition off a guest section of your system to limit damage for people who are not up to speed on the threat. Your company will need a rigorous approach to combat this problem, staying current with updates on a daily basis (Operating Systems, Browsers, PDF Readers, etc.). Ask yourself: How will we know if we have been attacked? To counter the threat you will need to address:

1. **Protection** – Start here and assume you will be breached. This includes a wide range of controls such as patch management, authentication controls, anti-virus blocking, and vulnerability assessments. Consider using a cloud provider that provides encryption for storing your data. And absolutely be careful about email messages and downloading any software; especially free games.
2. **Detection** – You will need to detect that you have been breached. This will require compliance monitoring, network alerts, Security Information and Event Management (SIEM) or Managed Security Service Provider (MSSP).
3. **Correction** – You must develop and practice an Incident Response Plan (IRP). If you fail to execute on your IRP, the data breach will get extended. Also consider outsourcing specialized expertise to support your IRP. For example, forensics is a special skill not commonly found in most organizations, but extremely valuable with effective responses.

"The world has become a playground for anyone who understands technology and is willing to bend the rules. By manipulating technology or people in unanticipated ways, an attacker is able to accomplish the seemingly impossible. This doesn't just include criminals, although the criminal element is huge, pervasive, and only increasing in efficacy – anyone can put in time to learn about our technology – warped world. We now live in an age where anything is possible." – Advanced Persistent Threat Attacking: The Art and Science of Hacking Any Organization by Tyler Wrightson

For bigger companies, it makes sense to create and resource a Chief Information Security Officer. If your company has outsourced software to other companies, such as Software as a Service (Saas), then make sure your contract allows for audits. This enables you to conduct your own tests to see if the vendor is up to speed. And if you don't act and follow through and you experience a breach, you can be found liable for negligence from the damaged parties.

This article has touched on a few basic points, attempting to raise your awareness. Your best defense is to be aggressive on the offense – make sure you have someone watching out for the bad guys. This includes hiring hackers to help build your defense. Also check with your bank, software vendors and other suppliers. They often have functions and features for security that many companies never choose to use. In today's environment this is a big mistake because sooner or later you are going to get attacked. Just look at what's happening to some of the biggest companies in the world.

"Everybody who uses cyberspace is at risk and it doesn't matter which type of computer or operating system you use. It doesn't matter whether you use a desktop, a laptop, a smartphone, a tablet or an online gaming console. The risk is inside the system. The risk is the result of a culture of permanent "always on" inter-connectivity. The risk is part of the huge growth of the internet in the last twenty years. Risk is everywhere in the digital world." – Cyber Attack: The Truth about Digital Crime, Cyber Warfare and Government Snooping by Paul Day