Securing Your Companyâ??s Cyber Security

Description

I recently met with the owner of a large real estate brokerage to discuss the scope and value of offensive security services. It was a great meeting and I thought they really understood the importance of protecting their network and digital assets. As we were wrapping up, they remarked â??I donâ??t think we need anything like that since we already have cyber insuranceâ?•. Really? â??No thank you Doctor, I will pass on the polio vaccination since I already have health insuranceâ?•. You get the point.

For decades, the title/real estate industry chugged along without giving much thought to cyber risks. Basic defensive measures were put in place (Antivirus, Firewalls, etc), and no news was good news. Well, we now know that title and real estate firms are some of the most targeted organizations out there! Why? Because hackers know that most of these organizations are not large enough to have sophisticated network security measures in place, despite handling millions of dollars in transactions every year.

So what now?

The first step in securing your companyâ??s cyber security posture is assessing where your weaknesses are. Putting effective defensive measures in place is great, but without understanding where you are vulnerable, this is like throwing darts. Start with a vulnerability assessment. A vulnerability assessment is a test that can be performed externally from your organizationâ??s network, within your internal network, or both, in an effort to identify as many different security vulnerabilities within your environment as possible. We can help guide you to identify and prioritize any weaknesses, thereby allowing you to implement a more effective defense.

Next, and probably most important, is to have every single one of your employees go through social engineering training. Phishing (email scams and click bait are good examples) is by far the most common form of social engineering and it is the easiest way for hackers to gain access to your workstations and network. We have all heard stories about buyersâ?? settlement funds ending up in the wrong place! Ever hear of Docusign? Dropbox? These are two of the most exploited programs out there. Oh, and by the way, both are widely used by both title and real estate professionals. Training is **SO** simple, yet **SO** critical (and we can do it via live and recorded webinars).

What is at risk?

A lot.

Non-Public Personal Information: Think about the amount of non-public personal information your company collects AND retains over the course of year. Consumer and employee information including settlement statements, mortgage information, 1099s, and social security numbers.

Escrow Accounts: What would happen if a hacker were to get their hands on all that money, which by the way, isnâ??t yours?

Software: What if someone were to compromise your software; whether it be settlement software, accounting software, transaction management software? Could they generate checks from your account? What else would they have access to?

Please donâ??t confuse this with fear mongering. That is not my intention. I simply believe we all have a responsibility to our clients, our employees, and ourselves, to take a proactive approach to protecting our data (and money).

Feel free to contact us at **FortyNorth Security** with questions or for a free consultation. We can customize assessments and/or training for companies of all sizes and budgets!

Here are a few good resources:

For Realtors: https://nvar.com/realtors/news/re-view-magazine

For Title Companies: https://www.alta.org/best-practices/

By: Jared Blatt
President & Co-Founder
FortyNorth Security

Category

1. Cybersecurity

Tags

1. featured

Date Created
2019/04/12
Author
vltaexaminer