



CYBER SECURITY

WHAT TO LOOK FOR & HOW TO SOLVE THE BREACH

CYBER SECURITY: WHAT TO LOOK FOR & HOW TO SOLVE IT



The real estate business is going more mobile and web-based each day. This means hackers are after the industry more than ever to steal money and information from you and your clients. We will review the different types of cyber risks and hacks as well as tips on how you protect your business.

93% of data breaches are traced back to employees opening emails or clicking links without verifying it.

#1 Phishing

We've all seen the HR emails and perhaps the news stories about this type of cyber attack. Phishing is a top concern when it comes to cyber security. Phishing is a deceitful online practice in which criminals pose as reputable companies in order to trick individuals to divulge personal information and private data. This info can range from: passwords, social security numbers, credit card info, and more. An example of phishing that has affected the real estate business are business email compromise (BEC) attacks where hackers will use emails in guise of a realtor, insurance agent, or any kind of business involved in the closing process to gain money or private data from the home buyer or even real estate professionals.

#2 Ransomware

Ransomware is an attack that locks businesses out of their network and/or data and won't release it until they receive payment, usually in crypto currency. It's virtual kidnapping in which you're not even guaranteed you'll get back what was withheld once a payment is made to these attackers.



What do you do if you've received ransomware?

Well, it appears the verdict is out on this one, with some saying you should never pay and others saying it may be worth it. To echo the sentiment of one of those articles: it's really up to you whether or not the cash is worth the loss. If you can recover the data and rebuild relatively quickly, while being able to take the hit to your business then it may not be worth paying the crypto currency. However, should it have anything to do with sensitive data involving money or personal information you definitely need to consider paying the ransom. Before you make any decisions however, you should seek legal advice and report these crimes to such places like the FTC's On Guard Online reporting system.

#3 Endpoint Attacks

Endpoint attacks are cyber strikes that prey on the weak access points that Software as a Service (SaaS), cloud storage services, and your unsecure personal device can be accidentally left vulnerable for hackers.

You may have heard of the "classic" attack when one drops infected USB drives in company parking lots so that an employee may curiously plug one into their work computer. However, many companies now rely on cloud-based software (like SaaS) to exchange and store files, images, and other important data. Such services like Google Drive and Dropbox can be vulnerable to data breaches, but also consider that apps on your phone like Spotify, Facebook Messenger, and Snapchat are SaaS with cloud storage that can leave you vulnerable.

Additionally, with the bring-your-own-device (BYOD) practice becoming more prominent and a basic need for those on-the-go in real estate, your device can become a gateway for cyber security attacks. Consider avoiding public wifi hotspots when working and invest in cyber security for your phone and computer!



TIP ON ENDPOINT ATTACKS!

Endpoint attacks on SaaS are a reminder that it's very important to never reuse a password on multiple login services, as one identical login can be used to hack into many accounts!



#4 Supply Chain Attacks

These kinds of attacks are also called “third-party” or “value-chain” attacks. These are attacks where your business is broken into through your partner, vendor or provider (that includes apps) that had access to your system and data. Supply chain attacks are one of the most frightening for companies, as they must trust in their partners and vendors to have a sound cyber security and a strong code of ethics in order to not have a security breach.

As a real estate professional, you must be careful in whom you trust and how much access they have to your data. Don't be afraid to ask about their own security measures before allowing access to your data. Remember, if you have a supply chain attack and your data is breached, customers will place responsibility on you for not doing your due diligence vetting partners and providers.

FACT!







Supply chain attacks happen more often than you think, from small to big companies alike.

Equifax blames their data breach from a supply chain attack through their software provider Image-I-Nation Technologies. In 2017, a casino's data was breached through their fish tank's high-tech thermometer.

12 Steps to Reduce Cyber Security Risks



Getting Started

PHASE ONE

-  Find Security Software
-  Secure Paper, Physical Media, and Devices
-  Control Access Points to Sensitive Data
-  Store Sensitive Data Securely and Protect It During Transfers
-  Segment Your Network and Monitor Who's Trying to Get in and Out
-  Secure Remote Access to Your Network

Developing Policies and Procedures

PHASE TWO

-  Require and Implement "Secure Passwords & Authentication" Policies
-  Establish a Plan of Action If Your Data Is Leaked
-  Insure You and Your Business Prior to an Attack

Additional Measures

PHASE THREE

-  Apply and Update Security Practices when Adding New Products or Data
-  Keep Up with Security Measures and Address Vulnerabilities
-  Make Sure Your Service Providers have Security Measures

When a Breach Happens, Here are 3 Actions to Take!



#1 Secure Your Business & Start Investigation

Contact Your Cyber Security Provider

Assemble a team of experts that may include, but are not limited to: Legal, IT, Human Resources, Communications, and Management. Consider hiring a data forensics team and legal counsel to understand the scope, source, and laws that have been breached.

Secure all physical areas related to the breach, take all affected equipment offline immediately, and close off all entry and exit points.

Remove data breach if it was improperly posted on your website and other websites, and contact search engines to ensure the breached personal information is not archived accidentally.

Interview those who found the breach and document their information. Inform all those involved at this point to not destroy evidence!



When a Breach Happens, Here are 3 Actions to Take!



#2 Fix Vulnerabilities

Do you know if service providers were involved in the breach? You may need to change the amount of access they have and how much data they can access. Be clear about the changes and why you are making them. Communicate these changes to providers and make sure they have fixed their issues as well.

Continue investigating and fixing security issues with specialists. For example, if you do not have a network where you've segmented it to one server, a breach will take over any servers that are not blocked off.

You need a comprehensive communications plan for all affected during a breach, like: employees, customers, investors, business partners, and other stakeholders. Don't withhold key details about the breach that could help those stakeholders protect themselves and their information, but also don't overshare - it may put them at risk. Do not lie or mislead with public or private statements about the breach either.



When a Breach Happens, Here are 3 Actions to Take!

#3 Notify Appropriate Parties



Follow legal requirements: A majority of the United States requires notification of security breaches involving personal information. For specific types of info and companies, you'll need to follow laws that apply to your breach and business.



Law enforcement: You must call your local police immediately. It's important for law enforcement to learn as much about the situation as possible. If your local police are not privy to investigating information theft & breaches, then you should contact your local FBI office or the U.S. Secret Service. (Mail theft needs to be reported to the U.S. Postal Inspection Service.)



Businesses: If specific account information (such as credit cards and bank account numbers) become stolen, you'll need to notify the company or institution so that they may monitor for fraudulent activity. If you stored personal information in any manner of another business, you need to notify them too.



Individuals: You'll need to notify customers, employees, and individuals whom have had their personal info compromised. They too will need to take steps to stop their information from being misused. Remember to clearly describe to them what was compromised and provide them with steps they can take to stop misuse. You can ask the police what helpful info to provide individuals so that it doesn't intrude on their investigation.



KEY TAKEAWAY

Cyber threats and security breaches are becoming more advanced and prevalent in the real estate industry and more.



norman-spencer.com

All content within the herein is the property of Norman-Spencer unless otherwise stated. All rights reserved. No part of the newsletters may be reproduced, transmitted or copied in any form or by any means without the prior written consent of Norman-Spencer.

The opinion(s) offered herein are intended for informational purposes only and are not intended to replace or substitute for any regulatory, legal, or other professional advice. Every effort is made to provide accurate and complete information which is error free. However, Norman-Spencer Agency, LLC, its parent, subsidiary, and affiliated companies and employees ("Norman-Spencer"), makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the contents herein and expressly disclaims liability for errors and omissions in such content. Norman-Spencer does not assume any legal liability for any direct, indirect or any other loss or damage of any kind for the accuracy, completeness, or usefulness of any information, product, or process disclosed herein, and do not represent that use of such information, product, or process would not infringe on privately owned rights. The content here is does not, and is not intended to, constitute legal advice or services. You should contact your legal counsel to obtain advice with respect to any particular legal matter.