HOW TO KEEP YOUR BUSINESS'S COMPUTER SECURITY SAFE FROM CYBER HACKS AND ATTACKS

By: Ben Hecht, Senior Director of Business Development, Kokua Technologies July 20, 2021

In the age of information, computer security is essential. The amount of damage a cyber-attack or hacker can inflict ranges from inconvenient to outright devastating. They're able to bring down an entire organization by targeting one key individual, and they're getting smarter about how they do it.

They aim for the beating heart of your organization namely, your finances. As a CPA (Certified Public Accountant), getting your house in order and ensuring you're up to speed on the latest threats to your security is paramount.

For this reason, this blog is going to focus on common computer security threats, how to identify them, and what practices to employ to remain safe and secure.

WHAT ARE THE COMMON TYPES OF SECURITY THREATS?

The Workforce
People aren't robots. They're human. And as humans, they're prone to making mistakes. Therefore, it's only prudent to set up a Security Awareness Training program to make sure your workforce is up to speed with the latest threats (both online and via email) and how to identify them.

Email Viruses
Ransomware is a common email threat. It's a virus that affects machines on your network by locking down specific files, drives or directories. In doing so, it renders them completely inaccessible and unusable. Sadly, they can only be recovered by paying a ransom – usually in the form of a cryptocurrency like Bitcoin or Monero.

These kinds of hacks have taken down massive organizations in the past. Consequently, they're a huge threat to small business owners, and especially to ones who don't have hundreds of thousands of dollars in ransom payments lying around.

Another email hack is in the form of phishing or spoofing campaigns. This is when a hacker sends emails from fake accounts with real employee names. They'll often include links that employees might click on by mistake, thinking they're doing the right thing. However, they'll end up installing a virus or paying money to the wrong person, which is why installing a spam filter on your domain can help to mitigate some of these risks – blocking some of the domains that shouldn't be sending you anything.

Data Breaches
Issues sometimes occur when confidential information about financial, legal or healthcare is sent over email

The foregoing information was furnished to us by sources which we deem to be reliable, but no warranty or representation is made as to the accuracy thereof. Subject to correction of errors, omissions, change of price, prior sale or withdrawal from market without notice. This article is for informational purposes only.
© 2021 WCRE All Rights Reserved

without either encrypting it or using a secure file sharing service first. This is especially problematic if a laptop is stolen or someone leaves it unattended for too long. If this information ends up in the wrong hands, it's game over for your organization, and this is especially true in the wake of GDPR. Consequently, it's important to keep your data as private as possible by encrypting all emails and drives.

Missold Computer Security Provisions

One of the biggest threats to CPAs (and to anyone for that matter) is misguidance. Therefore, when making decisions about IT services for your company, it's essential to know and trust where your recommendations are coming from. Hence why references are important. Don't let someone sell you something you don't need, and make sure your resource is thorough.

In short, ask the right questions and seek reassurances that the provider is concerned about their relationship with you first and foremost, not the dollar figure you're offering. Working with the wrong people and being misguided by them will only result in bigger issues further down the line.

WHY SECURITY AWARENESS TRAINING IS PERTITENT FOR STAFF AND BUSINESS OPERATIONS

It might surprise you to learn that the biggest threat to your organization doesn't come from an external source. It comes from your workforce. Shockingly, over 90% of cybersecurity incidents occur because an employee has been misguided into performing an action, such as accidentally clicking on a corrupt link.[1]

This is why providing a computer Security Awareness Training regimen, such as KnowBe4, can educate and help people identify cybersecurity threats before they accidentally do something that affects your entire system.

An added benefit of this training is how happy it makes your insurance providers! They like to know you're up-to-date on computer security – and so do compliance auditors, who will perform regular assessments of your environment to monitor your level of compliance. Due to this, it's essential to document all of your IT processes in your employee handbook. Make sure your employees sign off on an 'acceptable usage' and 'completion of training' certification on an annual basis.

Sadly, it doesn't matter how many security mechanisms you put in place. All of the planning can go out of the window if you don't know how to detect threats, which is why it's prudent to invest in security education. After all, one single click can bring down an entire company.

OUR RECOMMENDED COMPUTER SECURITY PROCESS FOR BECOMING COMPLIANT

At Kokua Technologies, we take a holistic approach to each of our client's projects. By identifying their unique needs, we can adapt our offer to ensure the best outcomes. However, that doesn't mean we don't have a tried and tested method that we know works.

"Building Successful Relationships" is our Mission.

The foregoing information was furnished to us by sources which we deem to be reliable, but no warranty or representation is made as to the accuracy thereof. Subject to correction of errors, omissions, change of price, prior sale or withdrawal from market without notice. This article is for informational purposes only.
© 2021 WCRE All Rights Reserved

It's worth noting that a cybersecurity plan is a collective effort. Working with IT, HR and insurance partners is essential for making sure things are properly addressed, modified, and supported on an annual basis. As the external threats continue to develop, so should the in-house procedures and measures that protect your company.

So, with that said, let's take a look at the process.

One: Work with your internal or external IT Partner to establish best practice standards for your environment.

From a high-level overview, these are some of the things to focus on:

- In-office & Remote Accessibility
- Secure File Storage & Secure File Sharing
- Data Encryption Policies
- Workstation Security
- Server Security
- Back-up & Disaster Recovery Plan
- Overall Network Security

Two: Document the best practices on how the company operates by developing:

- An Acceptable Use Policy
- A Remote Work Policy

Three: Work with HR to enforce policies based on this documentation.

Four: Work with 3rd party auditors/cybersecurity professionals to provide a specific audit to meet compliance needs.

Five: Ask the auditor to report the results to you and your IT resource.

Six: Work with your IT Team to 'button up the environment' based on the findings.

Seven: Update documentations & policies annually.

Eight: Make employees sign off on these policies annually.

Nine: Get a proper level of Cyber Security Liability Coverage that protects your organization in the event of an attack or security breach.

"Building Successful Relationships" is our Mission.

The foregoing information was furnished to us by sources which we deem to be reliable, but no warranty or representation is made as to the accuracy thereof. Subject to correction of errors, omissions, change of price, prior sale or withdrawal from market without notice. This article is for informational purposes only.
© 2021 WCRE All Rights Reserved

COMPUTER SECURITY BEST-PRACTICE TIPS

Network security doesn't have to be confusing. And although every accounting firm is built differently, there are tried and tested best practice tips that will help you mitigate risks from outside threats.

1. Provide a Security Awareness Training regimen for your organization to help them identify cybersecurity threats.
2. Consider a professional-grade firewall instead of using your internet service provider's gateway unit. This will protect your business with perpetually updated definitions, VPN access, and content filtering services.
3. Ensure your organization is accessing your company and client information from a secured device or connection, such as a VPN, remote desktop server or secure cloud environment.
4. Provide spam filtering for employee email communications for extra protection.
5. Implement a dedicated back-up appliance for your servers in the event something happens to your servers or files. (Cloud-based systems will often automate this).
6. Make sure you have a clear and robust continuity plan.

These are just a few top tips. However, once these security mechanisms and best practices are in place, the next step is to work with your HR department or consultant to create an Acceptable Use Policy and to document all the processes, security mechanisms and response plans in your Employee Handbook. If you employ a remote workforce, we recommend adding a 'work from home' policy to make sure employees aren't using the system in an unacceptable or dangerous way.

SHOULD I USE A SECURE CLOUD STORAGE SYSTEM?

If you have a physical in-house infrastructure, you've probably been approached about migrating your systems to the cloud. Let's take a look at some of your options.

Licensing Models

This is when you allow Microsoft Azure, AWS or Google to provide Infrastructure as a Service, which means you're turning your IT expenses into a manageable, predictable, and perpetual licensing model. Consequently, all the hardware, operating system upgrades, bandwidth, electrical, back-ups & redundancies, and most of the compliance requirements are managed by the experts behind the platform and handled in a single monthly payment. Scaling your organization is as easy as clicking a button to add more processing power, RAM, hard drive space and graphics processing power – all for a monthly bill increase.

Saas Environments

SaaS (Software as a Service) is predominantly a web-based cloud computing service and a common delivery model for most business applications.

"Building Successful Relationships" is our Mission.

The foregoing information was furnished to us by sources which we deem to be reliable, but no warranty or representation is made as to the accuracy thereof. Subject to correction of errors, omissions, change of price, prior sale or withdrawal from market without notice. This article is for informational purposes only.

© 2021 WCRE All Rights Reserved

Quickbooks Online is the most prominent example of a SaaS-based product used by accountants. The vendor will also host your data, handle all of the maintenance, cost of upgrades, and provide you with end-user support. The more you can push onto a SaaS host, the better. Check with your software provider if they offer a SaaS version of your product. If migration is within budget, it's worth it.

File Hosting Services

If you don't have servers for file storage, a great option to consider are secure file hosting services like Dropbox, Box.com, Onedrive or Sharepoint. It's important to save organizational files to a secure service or server and not store them on a local machine.

Summary of Cloud Storage Options for Computer Security

Although these cloud storage options are, arguably, more effective for larger-scale businesses, they're still worth considering for your client organization, regardless of its size. Because what you're really investing in is your client's productivity and operational safety. The greatest benefit of cloud solutions is how they keep your organization functioning in any possible scenario – without limitations. You're in a scalable, available, manageable, flexible, and reliable environment that will NEVER let you down. Because of this, increasing your monthly operational IT budget in order to protect your client company with features that enable top-notch remote solutions is an easy decision.

Also, after you move to the public cloud, you'll never have to pay for another server migration or replacement project ever again.

ABOUT:

Ben Hecht is the Senior Director of Business Development for Kokua Technologies, a managed IT solutions provider located in Berlin, NJ. Kokua is the Hawaiian word for help - and this dedication to support is the foundation of the company's impact for large multi-location firms, small one-location businesses, and residential users since 1989.

FOR MORE INFORMATION:

Ben Hecth
Senior Director of Business
Development 375 S. White Horse Pike
Berlin, NJ 08009
856.396.9240
Kokua Technologies

"Building Successful Relationships" is our Mission.

The foregoing information was furnished to us by sources which we deem to be reliable, but no warranty or representation is made as to the accuracy thereof. Subject to correction of errors, omissions, change of price, prior sale or withdrawal from market without notice. This article is for informational purposes only.
© 2021 WCRE All Rights Reserved