November 2014

TechTidbit.com

brought to you by Tech Experts

IT Policies Companies Under HIPAA Regulations Must Have

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

HIPAA (the Health Insurance Portability and Accountability Act) and HITECH (the Health Information Technology for Economic and Clinical Health act) have been around for quite some time.

Even so, many companies covered by these laws are way behind when it comes to implementation. When you really think about it, even companies not covered by these laws should have the requisite policies and procedures in place.

Access Control Policy

How are users granted access to programs, client data and equipment? Also includes how administrators are notified to disable accounts.

Security Awareness Training

Organizations must ensure regular training of employees regarding security updates and what to be aware of. You must also keep an audit trail of reminders and communications in case you're audited.

Malicious Software Controls

You must have documented policies for the frequency with which anti-malware and antivirus software are updated and what happens if an infection/outbreak occurs.

Workstation Use Policy

Requiring secure passwords, monitoring logins and limiting unsuccessful logins are just a few of the basics covered. Policies also need to cover basic security best practices such as not allowing passwords to be written down or shared with others.

Disaster Recovery Plan

How you respond to emergency situations (of all shapes and sizes) must be fully documented and tested regularly. A full Disaster Recovery Plan is something our company can help you with.

Media Disposal Policy

How do you dispose of old computer equipment and data? You must have policies and procedures in place that cover exactly how all equipment is properly disposed of and the disposition logged.

Review And Audit Procedures

There's much more to HIPAA compliance than the items discussed here; however, be certain also that whatever you do has a firm audit trail/log that shows that everything has been executed according to plan.

These are just starting points. If you're subject to HIPAA or just want to make sure that your company is covered by these simple best practices, contact our office and we'll be happy to review these areas with you.

Network Security And The "People Problem"

Michael Menor is Vice President of Support Services for Tech Experts.

Security teams that focus on what is already happening and the layers of defense being breached are constantly in reactive mode.

Reviewing reams of data produced by technology - firewalls, network devices or servers - is not making organizations more secure. With this approach, the team fails to prevent breaches or respond in a sufficiently timely way.

Instead, the addition of more data and more complexity perversely prevents achieving the end result: protecting sensitive information.

The significant breaches of today are executed by people infiltrating the organization and attackers are doing this by assuming identities or abusing insider privileges.

There is a gap between the initial line of defense (the firewall) and the company's last line of defense (the alerts received by the security team and their following analysis.)

Tracking user activity, especially connections between suspicious behaviors and privileged users, would allow organizations to close this gap.

True understanding of identity has the ability to cut through the overwhelming explosion of data that can render security organizations blind and unable to respond to real threats or even detect if they are under attack.

It is time to incorporate identity into the organization's breach prevention strategy and overall security. We have to stop accepting a gap approach to security, which is usually focused on data and devices rather than people. In light of the budding perimeterless world, identity will increasingly be the primary factor that matters to the security team.

Identity data is pervasive, yet typically absent from the security world view. For security organizations, our corporate identity (the personal identity elements we bring to our corporate environment) and our behavior are aggregate details essential in building a picture of what is happening within - and beyond - the corporate perimeter.

Together, they offer deep context to inform the security team of the appropriate response to potential threats and real attacks.

The critical piece in this approach is the security organization's ability and capacity to understand the full scope of identity: who the person really is behind any given device and whether they are behaving abnormally.

This is particularly helpful when identifying attackers that have managed to acquire privileged user credentials.

Identifying Normal Behavior

One way to reduce the scope is to focus on the highest risk identities first. If you accept that the greatest risk comes from people inside your organization that can access sensitive information – known as "privileged users", which can also include non-human accounts that may have access – then the correct steps are as follows:

1) Reduce the number of privileged users/identities and accounts.

2) Limit the privileges any one user has to systems and applications necessary to do their job.

3) Integrate the identities of privileged users into security and risk monitoring to spot behavior that may indicate a breach.

Closing the Gap

As more and more of the computing environment breaks outside of the control of central IT organizations, spearheaded by the move towards BYOD (or Bring Your Own Device), the ability to recognize who a user actually is and what is normal for them becomes a foundational part of effective security monitoring.

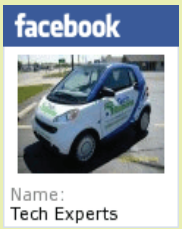
Without such identity-powered security, security teams will continue to struggle to differentiate whether the events they are monitoring are worth a reaction and that hesitation allows attackers to execute more and more damaging data breaches.

Furthermore, security teams will continue to operate in reactive mode and fail to prevent breaches or respond in a sufficiently timely way.

If identity is a central component to security management, then security teams will be in a better position to understand the behavior of users and will spend far less time trying to identify the meaning behind the events they are seeing.

People will continue to be our biggest point of exposure and with a keen focus on user behavior and activity, we will be in a much better position to limit the impact of breaches.

Visit The Tech Experts Twitter & Facebook



Our Facebook page is a great place to keep up with everything we're doing at Tech Experts! You can check out staff photos, press releases, blog postings, and enter our occasional contests! You can visit our page and become a fan at www.fb.com/TechnologyExperts

Twitter is another great place to keep up with everything going on at Tech Experts! You can follow us at www.Twitter.com/TechExperts

When Nature Strikes Part 2 – Fire In The Sky

Scott Blake is a Senior Network Engineer with Tech Experts.

Fires in or around server rooms and data centers can ruin your data and put your business at risk. It's a must to set up fire protocols when you build your room or building.

As I mentioned in Part One of "When Nature Strikes," the two most important protocols to have in place for any "in case of…" are 1) Have a Plan and 2) Secure Your Data. When dealing with the possibility of fire destroying your server room or data center, you'll want to make sure you also have Suppression, Containment and Insurance protocols in place as well.

Have a Plan

Disaster recovery plans are now becoming a requirement for many industries. To be prepared, businesses need to locate and define the regulatory requirements of their individual industry, which will also help avoid fines, penalties or negative press associated with noncompliance.

Trying to implement or even design a plan while in the middle of a disaster will only lead to a less than successful recovery. Make sure your team is ready for action and everyone knows what to do. It's better to be overprepared than have a plan that goes up in flames.

Secure Your Data

Back up your data regularly. Manage a duplicate copy of all data, programming, and company processes at a different physical location or in the cloud. That way, you can continue working at a secondary location if your system crashes. One way to do that is to keep copies of all your data, programs, bare metal backups and virtual machines in data centers in other states.

If you maintain data backups and business software on location, make sure you store them in a fire rated safe. Fire safes can be purchased anywhere from $100 to thousands of dollars for a fully-loaded safe.

Suppression

Fire suppression systems for server rooms and data centers are essential to the server room itself. A fire suppression system will automatically extinguish a fire without the need of human intervention.

Design standards for fire suppression systems for server rooms and data centers are carried out with strict guidelines as the fire suppression agents used can be dangerous if not designed correctly. Fires within these types of environments are suppressed in two different ways.

Reduce Oxygen - This method uses argon, nitrogen and sometimes carbon monoxide to displace the oxygen in the room. The objective of this method is to reduce the oxygen level to below 15% in the room. By reducing oxygen to this level, it will suppress the fire.

Chemical and Synthetic - Most chemical and synthetic fire suppression agents have some form of a cooling mechanism. These systems use less gas and maintain a higher level of oxygen. However, high doses of any synthetic or chemical agent can be toxic, so making sure your design is correct is absolutely necessary. Synthetic fire suppression systems will deliver its payload within ten seconds.

Containment

A fire doesn't have to be inside your data center to jeopardize IT equipment. Because radiant heat and smoke from fire in an adjacent room can be enough to damage sensitive network hardware, creating a protective barrier between your server room and the potential fire not only blocks indirect damage, but prevents flame spread as well.

Lightweight, flame-resistant ceramic panels can be used to build fire-safe archive rooms and data centers within larger, standard-construction buildings.

Insurance

Recovering from fire damage is expensive. Business insurance is crucial and it's not only for physical property. The right kind of insurance will replace lost income as well. Make sure your business insurance policy is up to date and has the correct coverage to support your business in crisis mode.

Make sure you have all of your suppression and containment systems built and installed by certified professionals. Insurance companies will require this in order for you to acquire the policy and even collect on it.

No one wants to get burned after a fire. Again, make sure your company insurance is up to date and has the appropriate coverage needed to rebuild your business.

If you have questions or you're looking for suggestions on prepping your business for recovery, not disaster, call Tech Experts at (734) 457-5000.

Contact Information

24 Hour Computer Emergency Hotline
(734) 240-0200

General Support
(734) 457-5001
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5001
(888) 457-5001
sales@MyTechExperts.com

Take advantage of our client portal!
Log on at:
www.TechSupportRequest.com

TECH EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5001
Fax (734) 457-4332
info@MyTechExperts.com

Consider These Great PC Upgrades

If you are in the market for a new PC, check out these tips on how to upgrade your PC and get more value for your dollars before you pull out your credit card.

A solid state drive

Nothing like an SSD to give you a more practical and noticeable performance increase. With more capacity and more chips and channels, you are guaranteed faster performance.

A faster CPU

You may want to add a new CPU if your computer is old and if the before-mentioned SSD does not entirely fulfill your needs.

Get more memory

With more memory, your operating system will spend less time moving data to disk and you will be able work with more open apps and large files.

Choose a larger display

While a touch screen might blow up your budget, you can opt for a 23-, 24-, 27-inch 1080p model for an affordable price and it will offer you a much better and productive computing experience.

Better gear: keyboard and mouse

Explore the world of wireless, wired, touch and ergonomic keyboard and mouse models and choose one that makes sitting at your computer a breeze.

After all, all our work is done with a keyboard and a mouse, and they need to be as much comfortable as possible.

Security Tips For Your Smart Phone

Today it is fairly easy to carry out business tasks using smart phones. Emailing, browsing the Internet and even creating or editing documents is now a breeze.

So technically, smart phones are now carrying a large amount of sensitive data that needs to be protected. Not only are Smart phones subject to the same threats as PCs, but they are also quite easy to misplace and lose.

Here are a few tips that will help you mitigate some of these security risks:

Screen lock the phone

Whenever you leave your phone unattended, lock your smart phone to require a password or PIN code or set it to lock after few minutes. This will prevent unwanted access and will protect your data in case the phone is lost or stolen.

Enable remote device wipe

Check if your phone allows the memory-wipe function in case it is lost or stolen. Some phones have this feature embedded, but most others will require that you download an app and potentially pay for the service that goes with it.

Apply system updates

From time to time, smart phone vendors, mobile carriers, or hardware manufacturers update the operating systems on their phones. These updates usually include useful and necessary security-related improvements.

Turn off Bluetooth discovery mode

Many people leave their smart phones on Bluetooth-discovery mode around the clock. On some phones, this feature is set by default; however, check your phone and make sure it is disabled when you are not using it. Failing to do so, your phone will constantly be discoverable to others and allow people to connect to your device without prior authorization.

Install mobile anti-virus

Malware purveyors are increasingly targeting smart phones. It is now important to use anti-virus software for your phone just like you would do for your PC.

This is particularly important for Android devices as they are built on an open platform susceptible to malware.

The latest in computer crash prevention: Computer Airbags