25 Essential IT Security Tips to Protect Your Business and Organization

by Michael Moran, Affiliated
www.aresgrp.com

AFFILIATED

Cybersecurity, Compliance, & Managed IT Support

Daily we see the headlines proclaiming the latest organization to have fallen victim to a hacker, virus, malware attack, data breech, ransomware, or some other denial of service hostage situation perpetrated by some nefarious “bad guys.”

When you look beyond the headlines, and read the follow-up articles on these breaches, often times interesting subplots and subtleties emerge indicating how these breaches were able to be executed.

Consider, if you will,

- In the recent Equifax breach that affected the personal data of over 140 million Americans. Do you realize that the company did not update a known, and recommended, security patch on a key web based application exposed to the internet?
- The breaches at Home Depot and Target did not actually penetrate their corporate security. The breach suffered by these organizations occurred by accessing their networks via small third-party vendors who had legitimate network access. These crimes of opportunity permitted the criminals to utilize vendor access to break in to the network and commence their data collection.

It appears that many times the “bad guys” are getting access by exploiting a **general lack of common sense** approach to systems and data security.

For more than 20 years, we have been involved in assisting our customers with implementing, managing, and securing their IT systems as part of their daily operations. The following **25 Essential Security Tips** report was created to arm our clients and their employees with the detailed know-how to drastically reduce their chances of becoming a victim of cybercrime. This report will provide some insight, and guide you as you think about your organization, your preparedness to prevent an attack on your systems, your organization, and ultimately, your bottom line.

Finally, at the end of this report, we’ve put together a generous offer I believe you will find quite valuable - please see the details at the end of this report. Reach out to us, and we will be happy to schedule a call, or arrange a meeting to discuss your interests or concerns.

We welcome the opportunity to help you achieve your business goals.

Mike Moran
President

michaelmoran@aresgrp.com
614.495.9658

CRN MSP 500 2018

AFFILIATED
Cybersecurity, Compliance, & Managed IT Support

25 Essential IT Security Tips to Protect Your Business and Organization

Your systems and data are vital to your organization, and you cannot afford to have your operations halted for days – even weeks – due to a hacker, virus, or malware attack.

Imagine having your bank account wiped out, your customer's personal data stolen, losing critical system data, or experiencing a systems outage for extended periods of time. Let's not forget the potential for bad PR, civil and criminal lawsuits, and hefty fines that can result from a data breach, or disruption of service attack.

This report is designed to provide you with a series of valuable tips you can readily implement to prevent attacks, intrusions, and phishing expeditions aimed at disrupting your operations. If you aren't prepared, you run the risk of being attacked before you have a plan in place to manage it effectively.

These are the specific areas where protocol needs to be established, so that your staff, and general business operations, are working to together to identify and prevent threats to the organization.

1. The #1 threat to your security is...

YOU! And your employees. Like it or not, we as human beings are our own worst enemies online, inviting hackers, viruses, data breaches, data loss, etc., through daily, seemingly innocent actions. In most cases, this is not the result of a malicious act; however, as a manager or owner, it is vital to monitor which websites your employees visit what files they send and receive, and even what they're posting in company e-mails. Choosing not to monitor could expose you and the organization to disastrous repercussions.

Even if only incidentally, the actions of your employees in the workplace can subject the company to monetary loss, civil lawsuits, data theft, and even criminal charges. Exposing the company to malicious code, disclosing confidential company information, transmission of pornography, are all actionable offenses.

One thing you can (and should) do is let your firewall help your people protect the company by configuring your firewall to document and monitor which websites users are visiting. Almost all enterprise-level firewalls have this ability built in; it is simply a matter of configuring the firewall and actively monitoring the reports. You are able to set the rules, write them into an Acceptable Use Policy (AUP), train your employees on what is and is not acceptable in the workplace, and have them signs and agree to abiding by the AUP.

2. Use STRONG passwords!

Thanks to powerful brute-force-attack software readily available online, hackers can try tens of millions of password combinations per second. Do you know that hacking software can guess a five-character password in under three hours? If you only use lowercase letters, that time drops to **11.9 seconds**!

You don't need me to tell you that you must have a stronger password that "password" or "letmein" to keep yourself protected. You KNOW you need a strong password, but what does a "strong" password mean? Characteristics of a strong password are:

*Minimum length of eight characters (longer is definitely better) *Contains a combination of uppercase and lowercase letters, numbers and symbols that are more challenging to guess.
*Don't use dictionary words with proper capitalization, they are a hacker's dream! (Password123#).

Even though the example above meets the requirements I just outlined, it's easily hacked. Keep in mind that these hackers have sophisticated password-hacking software that will run 24/7/365. **Here's a great password tip:** use a phrase that you can insert letters and numbers into, like $h@KeNb8ke.

3. New quarter, new password

We completely understand the challenge of remembering all the passwords for the many different sites, and sign-ins that we maintain, but this is a habit worth developing! Follow the calendar year when changing passwords to your online sites, financial/banking sites, and computer systems. We recommend you change these passwords at least once every three months, and it is critical that you don't reuse passwords, or use the same passwords for two different resources.

Imagine if your social media account gets hacked, you most certainly don't want the attacker to also be able to gain access to your Amazon.com and banking accounts as well, simply because you used the same password for both sites. Maintaining separate passwords is a lot of work – but the cyber-society we live in demands it.

As mentioned above, a good password will be composed of both lowercase and CAPITAL letters, numbers, and symbols (!@#$%^), and that passwords for various sites should always be different. However, you can make them similar (not the same), which will make them easier to remember. Try using J@nu@ry1! for site A, and J@nu@ry1@ for site B.

4. If this type of alert pops up, DON'T click on it!

You're working at your computer when suddenly – BAM! – you get what looks like a legitimate pop-up notification stating that your PC is infected, "click here" to run a scan or install anti-virus software immediately. This is a common scareware tactic used by hackers to get you to click, and therefore unintentionally download a virus. Remember – don't click these pop-ups; any reputable IT partner would NEVER deliver that information via this type of pop-up!

The issue is that these appear to be actual system alerts, or Microsoft operating system alerts, and look completely legitimate. Don't be fooled, NEVER click on the sites, or the pop-ups. Be safe and close your browser, not the pop-up window, but the browser itself. Clicking anything on the page or pop-up will trigger a virus download. If you are unable to close your browser, bring up your task manager (hold Control + Alt + Delete on a PC, and Command + Option + Esc to "Force Quit" on a Mac) and close the web browser or application where it appeared. Next, be sure to notify your IT department, or IT partner, to let them know what has happened so a truly legitimate scan can be executed to check for, and quarantine, any infections on your system.

5. How to foil ransomware

Not long ago, CryptoLocker, a ransomware virus, was all over the news for having infected over 250,000 computers in its first 100 days of release; we surmise that this reported figure falls short of the actual incidents as a result of this attack. Once executed, the threat is fairly straightforward: Pay us, or we'll delete all your data.

Ransomware, like the CryptoLocker attack, works by encrypting your files which prevents their use. Once the files are compromised, the hackers pop up a demand screen asking for payment ($400 to $2,000) within a specific time frame (e.g., 72 hours or three days) before they will release the key to decrypt your files. The last CryptoLocker virus forced many business owners to either lose data or pay up, since there was no other way to decrypt the files.

Diligent IT security is the best way to foil a ransomware attack. There are no absolute guarantees against infections, especially considering the hundreds of thousands of attacks being created daily. This is why maintaining a full, daily backup of your data OFF-SITE is a critical element to diligent IT security protocols! With a complete, off-site backup, even if you experience a ransomware attack, you are able to recover all your files without having to pay one thin dime. Remember to back up off-site PCs, laptops, remote offices, and third-party software data stored in cloud apps as well!

6. How to spot a phishing e-mail

A phishing e-mail is a bogus e-mail that is carefully crafted to look like a legitimate request (or attached file) from a trusted site. The purpose here is to get you to willingly give up your login information to a particular website, or to click, and end up downloading a virus.

Often these e-mails look 100% legitimate, and show up in the form of a PDF (scanned document), a UPS or FedEx tracking number, bank letter, Facebook alert, bank notification, etc. That's what makes these so dangerous – they LOOK exactly like a legitimate e-mail. So how can you tell a phishing e-mail from a legitimate one? Here are a few telltale signs…

First, hover over the URL in the e-mail **(but DON'T CLICK!)** and you are able to see the ACTUAL website to which you'll be directed. If there's a mismatched or suspicious URL, delete the e-mail immediately. In fact, it's a good practice to just go to the site directly by typing it into your browser, rather than clicking on the link within the message to get to the site. Other telltale signs are poor grammar, spelling errors, requests to "verify" or "validate" your login, or any request for personal information. Why would your bank need you to verify your account number? They should already have that information. Remember, if an offer appears too good to be true, trust your gut, it is too good to be true!

7. Bookmark LEGITIMATE websites you frequently visit

Here's a sneaky trick used by many hackers: they purchase and set up a fraudulent website that is a close misspelling of a legitimate one. Example: www.faceboook.com instead of www.facebook.com. It only takes an accidental "fat-finger" addition of ONE letter in the URL, and you're directed to a very legitimate-looking, fake copy of the site you were trying to reach. Additionally, the login and links, once in the site, are full of key-logger malware, and virus landmines waiting for you to click on them. This is particularly important to bookmark sites for any social networks to which you belong.

8. If you installed it, you must update it!

There are thousands of hackers who get up every morning with ONE goal in mind: to find a new vulnerability in commonly installed software (like Adobe, Flash or QuickTime) giving them access your computer. That's why companies like these frequently issue patches, and updates for KNOWN security bugs. However, once a KNOWN vulnerability is made public via a patch announcement, hackers work feverishly to figure out how to use the vulnerability to access those users who aren't diligent about installing updates. That's why it's important to update installed software programs as soon as possible.

Of course, if you have a trusted IT partner such as Affiliated, we're monitoring your network for these updates and handling them for you; but your home computers, smartphones and other devices that may NOT be under our protection probably need a little attention.

9. DON'T use public Wi-Fi until you read this

We're all guilty of connecting to free public Wi-Fi, whether we are at the coffee shop, hotel or airport, after all what's the harm in a quick e-mail check or surfing the web while you are waiting. BEFORE you connect to any free, public Wi-Fi again, make sure the connection is legitimate.

Commonly hackers will set up clones of public Wi-Fi access points, hoping you will connect to THEIR Wi-Fi over the legitimate one being made available to you. Take the time to check with an employee of the store, or location, to verify the name of the Wi-Fi they are providing, so you don't misstep and connect to the clone. Next, NEVER access financial, medical or other sensitive data while on public Wi-Fi, this includes online shopping online. You expose yourself to risk when you enter your credit card information via a public Wi-Fi, unless you're ***absolutely certain*** the connection point you're on is safe, and secure.

10. Help staff from unintentionally causing a security breach

With so many access points (cell phones, laptops, home computers) how can you keep their network safe from hackers, viruses and other unintentional security breaches? The answer is not “one thing”, but a series of things. Implementation and vigilance regarding installing and updating your firewall, antivirus, spam-filtering software, and backups. This is a full-time job, requiring specific expertise, which is our clients have chosen us to be their trusted IT partner.

Once a solid foundation is in place, the next item on your agenda should be creating the Acceptable Use Policy (AUP) that I mentioned in the very first tip. This includes TRAINING your employees: how to use company devices; to follow security protocols (never accessing company e-mail, data, or applications on unprotected home PCs/devices); how to create good passwords; how to recognize a phishing e-mail; and what websites to never access. NEVER assume your employees know everything they should about IT security - threats are ever-evolving and becoming more sophisticated by the minute.

11. Don’t just close your browser!

When accessing a banking site, or any other application containing sensitive data, make sure you log out of the site, and THEN close your browser. If you simply close your browser, some of the session information is still available for a hacker to use to gain entry to the site, and access to your information.

12. Your firewall is USELESS unless...

A firewall is a device that acts like a security cop, watching over your computer network to detect unauthorized access and activity – EVERY business, and individual, needs one in place.

However, your firewall is completely useless if it’s not set up or maintained properly. ***Consistency is key when it comes to your firewall.*** Applying upgrades, and managing patches requires attention on a continual basis, as does ensuring that your security policies and configurations are set properly. This is not a do-it-yourself procedure, but rather an area where you want to engage a trusted IT partner, such as Affiliated.

13. Remember: if you handle, process, or store credit cards

If you handle, process, or store credit cards in any manner, you are required to comply with PCIDSS, the Payment Card Industry Data Security Standards. You are legally bound to maintain a secure environment, and violation of these standards will result in serious fines.

There are various levels to these security standards, however don't get caught up in the notion that you really don't process enough to matter . . . the truth is you do! And conducting business, with your client's sensitive information, under the idea that "no one would want to hack us" is extremely dangerous. If you have clients that make credit card payments over the phone, or directly, you are subject to these regulations. Keep in mind that all it takes is an employee writing down a credit card number in an e-mail, or on a piece of paper, to violate the law; then you'll be facing legal fees, fines, and a reputation damaged when you have to contact your clients to let them know you weren't properly storing, or handling their credit card information.

Getting compliant – or finding out if you ARE compliant – isn't a simple matter which can be outlined with a 1-2-3-step checklist. It requires an assessment of your specific environment, and analysis of how you handle credit card information.

14. 3 rules to keep your data safe in the cloud

If you're using any type of cloud application (and these days, who isn't?), you are right to be concerned about data privacy and security. Are you aware that the company hosting your data is ultimately responsible for keeping hackers out of THEIR network, and that most cloud breaches are due to USER ERROR? That is why it is so important that you, the user, are savvy when it comes to security.

Here are a few easy steps you can take to improve your security in the cloud:

a. Maintain a STRONG password. I cannot stress this enough, which is why it bears repeating. Characteristics of a strong password include; being at least eight characters in length, containing both uppercase and lowercase letters, also containing numbers and symbols. Do NOT make it easy, such as "Password123!". While this does technically meets the requirements, it is a hacker's dream because it is so easily cracked.

b. Make sure the device you're using to access the application is secure. This is an area where you will need an experienced IT partner to install and maintain a strong firewall, updated antivirus, and spam-filtering software. Don't access your cloud application

with a device you also use to check social media sites, and free e-mail accounts like Hotmail.

c. "Reverse"-backup your data. If the data in a cloud application is important, then you must download it from the application, and back it up in another safe and secure location. That way, if your account is hacked, or the data is corrupted, you still have a workable copy.

15. If you've ever said this, you're ASKING to be hacked!

Want to know what every hacker hopes you believe? "We're small…nobody wants to hack us." This is the #1 reason why people (companies, specifically) get hacked: they dismiss the importance of IT security because they believe that "they're only a small business." This is not only a risky, and irresponsible excuse, but a small company will feel the impact of a breach more severely as it hits their bottom line.

One thing is for certain: NO ONE is immune to cybercrime. The facts show that one in five small businesses fall victim to cybercrime, a number which is increasing annually. More importantly, half of all cyber-attacks are aimed at small businesses, primarily BECAUSE they make themselves the low-hanging fruit, due to the vulnerability of inadequate, or non-existent, security protocols.

Here is one more critical point to ponder: If YOU aren't giving IT security the attention it deserves, how do you think your CLIENTS would feel if they knew about that? If for no other reason, you need to be diligent for the protection your clients' data, even if the only information you store about them is their e-mail address. Do you realize that if YOUR system gets compromised, hackers will now have access to your CLIENT'S e-mail, and can use that for phishing scams, and virus-laden spam? I'm certain you want to be a good steward of your client's information, and their privacy, and I'm equally certain that your clients feel the same way. Take the time, get serious, and put essential security practices in place.

16. Start with the basics!

You've heard these countless times: you must have antivirus software, and a strong firewall. However, today, there is more to security "basics" than a solid firewall. Consider the employee who uses their phone to inadvertently click on an e-mail from a foreign ambassador trying to move money to the US. They see it's a scam, but it's too late…that click infected their phone, and is now sending copies of every outgoing e-mail to a foreign crime network.

Have you taken the time to train your employees? How do they react when they receive an Excel attachment named "Invoice" from someone they don't know? A single crack in your internal armor can open the door for invasive network attacks. Get serious about locking down your devices, e-mail filtering, and educating your users.

17. Routers are $100 at big-box stores – why do I need a $900 firewall, AND then pay an annual maintenance fee?

Routers and firewalls can be somewhat confusing – essentially, they serve the same purpose of distributing Internet to devices on the network. However, they work in very different ways. A router, like you'd purchase at a big-box store, is designed to serve the needs of home connectivity, not business connectivity. In a home environment, it's likely more important that the Xbox has a great Wi-Fi signal, rather than being able to deny all Internet access from North Korea. A firewall, unlike a router, is intelligent, and assesses all internet traffic passing through it to determine its legitimacy, that it was requested from an internal computer, and is not a virus. You typically pay a subscription fee, because the firewall is constantly updating itself to protect against the newest cyber-attacks. They also allow us to totally block access to some third-world countries known for producing cyber-attacks. A good firewall can also let you know what your staff has been up to – who's that looking on careerbuilder.com for five hours? Don't cheap out, and don't buy your business's gate to the Internet from a big-box store. It truly is the gateway between your business and the rest of the world – you need an intelligent armed guard, and not a robot incapable of identifying a threat. If you can afford to invest in only one thing, get a good firewall!

P.S. – Business-grade firewalls can be used in homes as well – especially if you want to control the content users can access on the Internet, and want to see what the people in the house have been doing. There is no rule that a firewall is just for business – we sell them for use in the homes of many CEOs, CIOs, and other professionals.

18. The long-forgotten piece of security for road warriors...

Do you connect to the office network, or VPN (virtual private network), to get some work done in the evenings, on the weekends, or when you're on the road? For many of us, the answer is yes.

One of the most frequently overlooked components of network security is ensuring that personal devices used to connect to the office conform to your organizations security standards. Make sure all your road warriors, and remote workers, have up-to-date antivirus software on the devices they use to connect to the office, and that, when at all possible, a good firewall is in use. Just know that it's generally safe to connect into work from public hotspots, as long as your office VPN is in use. The VPN secures the connection between the computer and the office. Remote login software such as GoToMyPC, and others, may not use the same type of security as your VPN, and therefore may not be safe to connect from a public hotspot.

19. Physical security matters!

A recent incident reported in US News accounted an office secretary unknowingly releasing some of her law firm's most private data to a gentleman who appeared to be from Comcast Cable. Dressed in a Comcast Cable polo shirt he bought on eBay, khaki pants with a tool belt, he told the secretary he was there to audit their cable modem specifications, and take pictures of the install for quality assurance.

She had no reason to suspect he was part of a now-extinct hacker ring, or that by gaining access to the office, he would also gain access to the business's private by noting the configuration details and passwords, for their firewalls and cable modems. In some cases, criminals were actually able to build a secure VPN private backdoor which they later used to steal data. If someone dressed up in a utility-provider uniform, would you let them in?

Ask for identification, and to whom they have spoken regarding the service they are performing. It is perfectly acceptable to be gracefully suspicious. Do you have a company policy in place documenting how visitors are permitted access to the building? If so, it is important that your employees are operating within those policies; if not, then this is a real problem your office needs to address, and you will need to work to define an access policy.

20. Don't just send your private information to anyone!

We're seeing a new variant of an old scam. Here's how it is executed: a secretary gets an e-mail from their boss – who is traveling – requesting that, as soon as possible, please send scanned copies of all the W2s the company issued at the end of January. The message appears to come from their manager, including having what looks like their actual e-mail address when viewed in Outlook. Yet the secretary is suspicious – having spoken to their boss on the phone that morning, there was never any mention of needing that information. Before collecting the W2 PDFs that are on the HR drive, the secretary decides to text the boss and verify the request. Great catch! The boss never requested that information. Had the secretary not been proactive, and instead just completed the assigned task, all of the confidential information that is on a federal W2 form for every employee in the firm would have been inadvertently provided to a scammer! That scammer would likely have used the information to commit identity theft and/or file false returns next year to claim any refunds.

Always be vigilant and proactive – it's better to be suspicious and double-check everything when dealing with confidential information. If necessary, provide that detail in an encrypted e-mail, or at minimum with a password on the files (and never include the password in the body of the e-mail!). The few extra minutes it takes could save months of heartache for all of your employees. Remember, if it doesn't feel quite right, it probably isn't – trust your gut!

21. Don't just throw out that old computer

Getting rid of old computers or servers? Did you know that the components used in technology equipment are not landfill-safe? On top of the environmental hazards, unprotected e-waste typically contains a lot of confidential, private information in the form of saved passwords, Internet history, and files left on the retired computer or server.

The first step is to find a local recycling facility where you can safely dispose of e-waste, then be sure to take the **#1 security precaution** before you haul it off: remove and destroy the hard drives. A drill and hammer usually do the trick just fine. Alternatively, many companies that shred paper documents will also provide services to destroy your hard drives.

Don't forget other e-waste such as ***mobile phones, printers and copy machines***, and any other device that ever touched your company data. Give serious thought to what data is on any device before you recycle it.

22. Basic cybersecurity training

Think fast: what's the first thing you do after realizing you just opened an e-mail from the Nigerian prince wanting to give you a sum of $34 million? You didn't reply, which is great, but do you realize that the threat still remains. Do you know what to do immediately upon discovering a virus, e-mail threat, or other cybersecurity issue?

You need to have step-by-step instructions detailing what to do if employees believe they have witnessed a cyber-incident. Training needs to happen NOW – not when the problem is happening. A simple training program can be very effective, including items such as: physically disconnecting the machine from the network (or the power from the machine), notifying your trusted IT partner of any suspicious e-mails or unusual activity, and procedures to follow if you lose your mobile device. These are all part of a simple yet effective employee cybersecurity plan.

23. Do you allow guests to access your Wi-Fi network?

Do you have guest access on your company Wi-Fi network? Or do you simply give out the same password that your employees use? If you give out your password, you're practically opening the door for anyone to come in and steal private information, infect your private computers, and even steal customer credit card data if you are processing them over the same Internet connection.

The key to providing free guest Wi-Fi access is in segregation and security. Your Wi-Fi guests need to be completely isolated from your private network. Your guests should not be able to reach your internal computer network, credit card terminals, or other network-connected devices. Don't know how to enable guest Wi-Fi access? As a trusted IT partner, Affiliated is positioned to provide these services.

24. Should my computer be encrypted?

It's another Tuesday in the airport, you just cleared the TSA line, and went to the pretzel shop for a quick bite before you catch your plane. You sit your laptop down to get a straw, and the next second…your laptop is gone. It's not in sight, nor is the thief who stole it.

If you have a password on your laptop, that will likely prevent the thief from immediately having access to your private documents. What it doesn't stop is someone removing the hard drive from your laptop and connecting it to another computer – suddenly your hard drive is sitting there, ready to browse – just like any other folder or drive.

What should you have done? ***Encrypt it!*** A good first step toward protecting the hard drive of your laptop, and other mobile devices, is to encrypt them. With the drive encrypted, a thief can't just pull it out, hook it up, and suddenly have access to all your files. At least you've made it difficult for them to get to your data.

25. Is it time for cybersecurity planning?

The time to start planning for a security threat isn't during a virus outbreak, or immediately after you discover funds transferred from your banking accounts. Decisions and judgments made during this time are typically driven by emotion, and are felt under extreme pressure. Missteps can be made, that having a plan in place would have allowed you to avoid. The time to make cyberthreat plans is now.

Things to consider when you're planning:

- Physical access to your building(s)
- What to do with lost or stolen mobile devices
- PCI (payment card industry) compliance requirements
- Data-breach incident response
- Threat monitoring

There are some great resources out there for businesses that just don't know where to start with cybersecurity. Take a look at http://www.fcc.gov/cyberplanner for a customizable guide to get started with operational and organizational planning. Keep in mind, that as a trusted, experienced IT partner, Affiliated can help you evaluate your "cybersecurity" plan.

How Affiliated Can Help

To help you protect your systems and be prepared for potential issues, Affiliated is offering you and your organization a FREE Review Of Your Existing Security Systems, Procedures, and Practices. This no-obligation review will identify areas that may be an issue now, those that could be problematic as you prepare your plans for the future, as well as show you how to align one of your key assets more closely to your business goals.

We will meet with you to review your existing systems and plans, and make recommendations on ways to ensure that your team can avoid pitfalls, prevent intrusions and denial of service attacks, and recover quickly and effectively in the event of an attack.

To request your review, call our office at (614) 495-9658 and ask for Jason. He will personally follow-up to schedule your Free Security Review. Or send me an e-mail at michaelmoran@aresgrp.com**.**

The Channel Company's CRN Managed Service Provider (MSP) 500 annual list distinguishes the top technology providers and consultants in North America whose leading approach to managed services enables their customers to improve operational efficiencies, realize greater value from their IT investments, and successfully leverage technology to achieve greater competitive advantage.

CRN MSP 500 2018

AFFILIATED
Cybersecurity, Compliance, & Managed IT Support