

# MTC TECH TALK

*For Humans  
Not Geeks!*

Your resource for the latest technology updates and opportunities for your success.



## How to Improve Security and Build Customer Trust with Cybersecurity Assessments


### What's In This Issue?

Your Monthly  
Technology Update

A Four-Day Week Doesn't  
Mean Four-Day Security

Are You Being Watched?

Don't Forget Your Phone Security

Meeting Tree Computer  
 (845) 237-2117

In the age of ever-evolving cyber threats, organizations can't afford to be complacent when it comes to security. Whether you're a small startup or a large corporation, cyber-attacks can cause significant damage to your reputation and bottom line. This is why it's crucial to take the steps necessary and mitigate risks as much as possible. A cybersecurity assessment is one component of a robust security strategy that doesn't often get discussed.

Put simply, a cybersecurity assessment is a comprehensive evaluation of your organization's security measures which aims to identify vulnerabilities and weaknesses in your network, applications, and systems that cybercriminals can exploit. By identifying and mapping these weaknesses, you can proactively improve your security and prevent potential data breaches and other cyber-attacks.

But the benefits of a cybersecurity assessment don't stop there. If your organization handles sensitive information, such as in the healthcare or finance industries, you may be subject to strict regulations. By conducting regular assessments, you can ensure that you meet these requirements and avoid costly penalties for non-compliance.

Moreover, a cybersecurity assessment can help you build trust with your customers. With data breaches becoming more common and publicized, many consumers are increasingly concerned about the security of their information. Regular assessments demonstrate your commitment to protecting your customers' data and show that you take security seriously.

There are many types of cybersecurity assessments. However, here are a few that you may have heard of:

#### Penetration Testing

Penetration testing is a cybersecurity assessment that simulates actual, real-world cyber-attacks. Pen tests are usually performed by an experienced team of ethical hackers who use various techniques to exploit (known) vulnerabilities and aim to validate how easily an attacker could breach your systems. Just like a cat trying to catch a mouse, the hacker will try to find weaknesses in the system and fake exploit them to gain access to sensitive data on our system.



As you can imagine, Pen Testing isn't cheap and can cost anywhere between \$4000 and \$100,000, depending on the size of your company and the complexity of the network. On average, a high-quality, professional pen test will run between \$10,000 and \$30,000

### Vulnerability Assessment

Where pen testing is a detailed hands-on examination by a real person trying to detect and exploit weaknesses in your system, a vulnerability scan is an automated, high-level test that looks for and reports potential vulnerabilities in your company's network, applications and systems that hackers could exploit.

In this particular assessment, a team of experts scans your IT network systems using automated tools designed to detect a wide range of vulnerabilities, including outdated software, weak passwords, open ports, and misconfigured systems.

Once completed, the team will present you with a report outlining any vulnerabilities found. It will prioritize each weakness that needs your (your IT partner's) attention to improve security and reduce your risks.

### Security Risk Assessment

A security Risk Assessment is a technical assessment, or audit, of organization policies and controls. The assessment evaluates your organization's security posture against industry standards and compliance requirements.

This audit usually takes the form of a questionnaire and should be conducted annually, mapping your current security posture and comparing it to security industry standards such as HIPAA, SOX, NYDFS, CMMC, etc.

These are some of the questions you might be expected to answer in this type of assessment:

1. What are your IT security best practices?
2. Do you have an established plan to address security breaches?
3. How confident are you of your ability to demonstrate compliance?
4. What kind of hardware/software/process are you using to detect, intervene and terminate the operation of highly dangerous malware, such as ransomware?
5. Who has access to your data and your IT system, both in-house as well as from the outside?

If and when it becomes clear that there are security gaps in

your processes and systems, it's critical to work with your IT support partner to prioritize them and create a time-scheduled remediation plan.

### Third-Party Assessment

Finally, a third-party assessment. This assessment evaluates the security measures implemented by your vendors, suppliers, or other third-party partners that have access to your sensitive information and systems, like an outsourced HR partner, CPA, or cloud provider. The assessment ensures that these third parties implement adequate security measures to protect the company's data and systems.

More and more often, hackers target third-party partners as a way to gain access to their larger target organization. Remember Target? Attackers used a third-party vendor's access to compromise their network and steal sensitive customer information.

By conducting third-party assessments, you can identify and address potential vulnerabilities in your supply chain before something goes wrong. Similar to a Security Assessment, this audit is usually in the format of a questionnaire and focuses on your vendors' policies, processes, and procedures so you can determine the additional risk they pose to your organization.

After each vendor completes the assessment, you'll need to examine their answers and analyze the results. This will help you understand how much risk you'll take on when working with them and allow you to take appropriate steps to address potential concerns.

In rare cases and high-risk situations, you may need to remove a particular vendor from your list altogether.

Hackers are constantly trying to break into your computer system and will use whatever vulnerability they can to gain access. More than 11 billion records were stolen between 2008 and 2020, and the number's only increasing. By investing in regular cybersecurity assessments, not only are you improving your overall security and mitigating potential risks, but you are also taking proactive steps toward ensuring your customers that you have their best interests at heart.

Remember, if the hinges are missing, a lock on the door does nothing to protect you. Assessments allow your IT partner (us) to test all the doors, windows, and hinges before hackers have a chance to break in. Don't wait until it's too late - take proactive steps to protect your organization and call us today.

## Technology Update



### Did You Know... About Microsoft Edge Flags?

Microsoft Edge flags are an experimental feature that can enhance your browsing experience. They make scrolling smoother, enable multiple items to download at once, and even allow you to choose a color profile for your browser. The risk is that some may not work all the time, but in exchange, you get a boatload of new features before normal users will.

Accessing the flags menu is super easy. Enable them by typing `edge://flags` in your address bar and selecting the flags you'd like to try.

---

# A Four-Day Week Doesn't Mean Four-Day Security

Are you one of the many companies around the world that's looking at a four-day working week? Perhaps you've already made the leap.

For lots of businesses, it's never going to work. But many that have tried it have found it to be hugely positive.

But it has to be done right.

Forcing people to cram the same amount of work into fewer hours could lead to corners being cut, which in turn could lead to a cyber security disaster as human error due to a lapse in concentration becomes inevitable.

According to the World Economic Forum's 2022 Global Risk Report, nearly all cyber security issues can be traced back to human error.

So, what does that mean for your business?

If you're considering a four-day week, work closely with your people to make sure they aren't experiencing additional pressure.

Never assume that fewer office hours means you can relax your cyber security. You should reassess your measures to make sure they stand up to the change in working patterns, but also revisit your policies so that all routine tasks are still accounted for in the new working week.

Comprehensive security policies become even more

important when you change a work routine, and you may also want to beef up your approach.

Consider introducing 'zero trust' strategies if you haven't already. These give people access to only the files, software, and systems they need to do their job – and nothing more.

Finally, refresh employees' cyber security awareness with regular training. If security practices are not followed, it's often because they are not fully understood.

There's a lot to think about, but professional advice is always on hand.

If it's something you're considering, just get in touch.



## Are You Being Watched?



What else do you get up to when you're sitting in front of your laptop, working from home?

Perhaps you like to snack. Maybe you have the TV on in the background. You may even have someone else with you who's also working from home.

How would you feel if a stranger was watching? Creepy idea, right?

It's a real possibility if you have a built-in webcam. Undetected malware could be keeping tabs on you and your home, so it's a good policy to disable your webcam when you're not using it, and only allow the apps that need it to have access.

In Windows OS:

- Choose Settings from the Start menu.
- Select Privacy.
- In the Camera section choose 'Allow apps to access your camera' then move the sliders for each app on or off.

In Mac OS:

- Choose Apple menu > System Settings, then click Privacy & Security in the sidebar. (You may need to scroll down.)
- Click Camera.
- If you don't see Camera, upgrade to macOS Mojave or later.
- Turn access to the camera on or off for each app in the list.

An alternative to this is to buy a webcam cover for your laptop. That's ultimate peace of mind.



# Don't Forget Your Phone Security

It's common for people to rely on their personal phones to keep in touch at work.

That's not always the best idea, and there are lots of good reasons to provide company phones to your team (would you want to own the number and block access to sensitive data if somebody left?)

But regardless of who owns the device, you need to make security your top priority. Cyber criminals know how much valuable information lives on our mobiles, and they're making phones a target.

Here are our top 5 ways to keep phones secure:

## Set Minimum Upgrade Requirements

Cyber crooks and device manufacturers both work in three-year cycles. That means that, as threats evolve, so do the protections that address them. Upgrade devices to follow this cycle, and even if you're using BYOD (bring your own device), enforce this rule

if employees want to use their personal phone for work.

## Implement Mobile Device Management

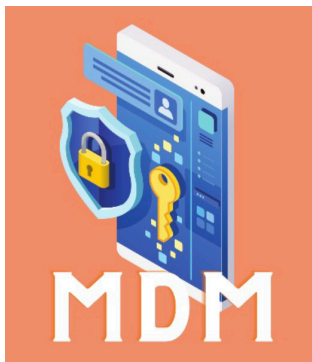
MDM allows you to track the location of devices, lock/wipe their data remotely, and can help you access remote support for any issues. That means your data stays safe, even in cases of a lost or stolen phone. You can also create a list of apps that are to be blocked for security reasons.

## Set Up MFA (Multi-Factor Authentication)

Make sure all devices have biometric locks requiring facial or fingerprint ID to open them, and that all apps require MFA to log in. Only allow employees access to the software and files they need for their job.

## Always Update Everything

Like all your devices, phones need to have the latest updates installed as soon as they become available. If you have



MDM in place, it's possible to schedule updates across the entire team at the same time – ask us for more info.

## Regular Awareness Training

You should hold regular cyber security training for your team that includes mobile devices. Your people are your weakest link when it comes to security. Keeping them up to speed on security risks can improve compliance.

It's easy to overlook mobile devices when it comes to keeping your data secure, but it's a vital step in protecting yourself against cyber attacks. For any help or advice, get in touch.

# Q&A

I've deleted an important file – can I get it back?

If you've checked your recycle bin and it's not there, don't panic. As long as you have a working backup, your file should be recoverable. Just don't do anything else... call an expert (we can help).

Why do I keep losing connection to the office Wi-Fi?

It may be that your router is overloaded. Restart your device and try again. If that doesn't work, try connecting on another device – this should tell you if it's a device or router issue.

I've noticed a new Admin account appear on my network. How did that happen

If no one in the business has created this account, you may have an intruder in your network. Contact your IT support to investigate it immediately.

## All Businesses Should Adopt MFA. Now



Multi-Factor Authentication (MFA) means you need at least two pieces of information to log in to a device or an app. Perhaps a password plus a fingerprint, and possibly an extra, single-use code sent to your phone.

Cyber criminals use increasingly sophisticated techniques to bypass security. So the more barriers you put in their way, the harder you make it for them to break into your systems.

All businesses should be using MFA as it provides great protection against cyber-attacks and other security threats. [Our new free guide tells you all you need to know.](#)

Ask us for a hardcopy today: 845-237-2116.

**Submit Your Questions Here:**  
[info@meetingtreecomputer.com](mailto:info@meetingtreecomputer.com)

## This is how you can get in touch with us:

call: 845-237-2117 | email: [info@meetingtreecomputer.com](mailto:info@meetingtreecomputer.com)  
website: [www.meetingtreecomputer.com](http://www.meetingtreecomputer.com)



Follow Us

