How to Have the Comfortable Cybersecurity Conversation with Your Technology Team

2023 Edition

Quest TECHNOLOGY GROUP

It's a Different World Today

Today's companies, regardless of size, have one important thing in common –their day-to-day security needs are very different than they were just a few years ago.

It's hardly news to anyone that the way we work has changed. We have moved from the relative safety and control of our company's physical four walls to a borderless frontier.

And with this shift the reliable technology services we came to depend on are no longer adequate.

How Your IT Support Needs Have Changed

Every company has someone responsible for planning, implementing, and supporting its IT needs. Whether outsourced to an IT provider, delivered by an internal team, or a combination of the two, now is the right time for a conversation with your IT team.

Let's assume for a minute you have outsourced at least some of your IT services to a third party. What does your agreement with them include? Often, you will hear them say "W*e take care of all your IT needs*."

That feels reassuring, doesn't it?

This might have been good enough when "all" you needed were reliable server backups, a reactive anti-virus, and Windows updates.

Those days are behind you.

As a customer, you might reasonably assume "all" extends to today's proactive monitoring and remediation from cybersecurity breaches. Traditional managed services providers (MSPs) are often not skilled in today's cybersecurity defenses your company expects and needs.

This leaves a widening gap between what is described as “your IT needs” and what you reasonably assume you are receiving.

What About Your Internal Technology Team?

Like an outsourced IT provider, your internal team needs to be part of the conversation. The questions you ask might be slightly different, but the need to align expertise with cyber risk is the same.

It is not uncommon for internal IT teams to focus primarily on day-to-day support. Unless your company has a formal program in place to develop solid new cybersecurity skills, you will find these skillsets are lacking.

Hiring experienced security team members can be costly and difficult. The demand is high and availability low for this specialized skillset. The functions they perform are different than the internal operations support your core IT team delivers. Think of these security team members as a new addition to the company toolkit.

To fill in the skills gap within your internal team, outsourcing and partnering are practical alternatives.

What a Typical IT Support Team Looks Like Today

There is no one size fits all requirement for the right technology support team. This chart includes many of the day-to-day needs a company has.

Take a few minutes to review these. Check the ones that apply to you now.

As you work through this, you will likely discover responsibilities you had not considered before. That's perfectly okay. This is your opportunity to create the IT support organization that meets your current and future needs.

Responsibility	✓	Internal IT	✓	MSP	✓	Network Security	✓	CIO
Day-to-Day User Support								
"It doesn't work"		•						
"How do I..."		•						
Help desk level 1		•		•				
Help desk advanced						•		
SOC help desk						•		
User Management								
IT-related onboarding steps		•				•		•
IT-related offboarding steps		•				•		•
Add and remove network users		•						
Active Directory maintenance		•				•		
Group Policy management						•		
Hardware Management and Support								
Define, implement, manage user-owned devices						•		•
Define, implement, manage company-owned devices						•		•
Define, implement, manage remote work policies						•		•
Define, implement, manage equipment acquisition policies						•		•
Research, recommend equipment		•				•		•
Setup new desktops, laptops, printers		•						
Setup new internal servers		•		(1)				
Configure for Windows updates		•						
Configure based on company policies		•						
Monitor for company policy compliance						•		•
Support company-approved user-owned devices		•						

Responsibility	✓	Internal IT	✓	MSP	✓	Network Security	✓	CIO
Troubleshoot, repair desktops, laptops, printers, servers		•		(1)				
Maintain firewall firmware updates		•						
Install routers, switches		•		•				
Monitor disk usage alerts		•						
Software/Application Management and Support								
Participate in software/application review, approval		•				•		•
Define, implement, manage software acquisition policies								•
Review, approve vendor solutions		•				•		•
Setup new user email account		•						
Setup new user hosted applications account (ex. Office 365, G-Suite)		•						
User support for approved applications, software		•						
Monitor for non-approved software installs, downloads						•		•
Support internal development team		•				•		•
Monitor third-party application updates, vulnerabilities						•		•
Backup Management								
Review, approve vendor solutions		•				•		•
Define company backup, recovery, retention policies								•
Configure internal network backups		•		•				
Monitor daily backup activity		•		•		•		•
Resolve backup issues		•		•				
Configure hosted application backups		•						

Responsibility	✓	Internal IT	✓	MSP	✓	Network Security	✓	CIO
Monitor hosted application backup activity		•						
Resolve hosted application backup issues		•						
Security Management								
Define, oversee company security policies, processes, procedures with C-suite		•				•		•
Understand cyber insurance terms, condition, exclusions		•				•		•
Regularly communicate, educate company security policies to all employees						•		•
Conduct network discoveries						•		•
Conduct vulnerability assessments						•		•
Conduct penetration testing						•		•
Conduct compliance assessments						•		•
Conduct Security Awareness Training						•		•
Security policy management						•		•
Access control management						•		•
WAN security configuration/ management						•		•
Advanced firewall configuration/ management						•		•
Network traffic monitoring						•		•
Password policy configuration						•		•
Risk management						•		•
Risk analysis calculations						•		•
Data Management and Governance								
Define, implement, monitor data security policies and procedures						•		•
Create, maintain company data mapping						•		•

Responsibility	✓	Internal IT	✓	MSP	✓	Network Security	✓	CIO
Define data access roles, rights		•				•		•
Implement data access roles, rights						•		
Monitor data access activity						•		•
Perform regular PII/PCI scans						•		•
Monitor data collection, storage, disposal						•		•
Asset Management								
Create hardware inventory		•				•		•
Create software inventory		•				•		•
Maintain hardware inventory		•				•		
Maintain software inventory		•				•		
Manage equipment disposal according to company policy		•				•		
Risk Management Policies and Procedures								
Create company security policies		•				•		•
Get legal approval for company security policies								•
Monitor security policy compliance						•		•
Deliver regular compliance reports to C-team						•		•

Why Have This Conversation Now?

There was a time not so long ago when small and medium-size companies believed cyber attacks were reserved for the big companies with something substantial to steal.

This is no longer true. In fact, the number of attacks and breaches against SMBs --- and this includes MSPs ---is continually increasing.

Why? For several reasons including –

It's easy.

Of course smaller companies don't have the data that big companies do, but they also are lacking the security defenses of their large counterparts. This makes SMBs low-hanging fruit for hackers. While the payday isn't nearly as large, the ease of acquiring data that can be resold makes the breaches worthwhile.

MSPs have a single point of access to many companies.

If that isn't reason enough, then consider that MSPs – the very IT support resources you might rely on --- are seeing an increase in cyber attacks. Again, the reason is obvious. MSPs have access to many companies' networks. The path to compromising many companies with one MSP breach is a short one.

Cybersecurity Protection Can Be Simple and Cost-Effective

We too often hear business leaders describe cybersecurity as "complicated" and "expensive". Let's put both of those concerns to rest.

Complicated happens when technology service providers don't explain technology concepts in plain English. That's why we have created The Questionary.

We understand how frustrating technology can seem, and we know it doesn't have to be. Our mission is to give you the knowledge you need to make informed, confident decisions for your company.

And then there is **expensive**.

We believe every company deserves proper cyber protection. We're a small company too so we understand how carefully you need to manage your budget. Investing in technology and tools that you can't touch, see in action, and measure an immediate return feels questionable.

But we know firsthand how critical these tools are for your company. In fact, we have invested in each of these ourselves. That's how committed we are to delivering the same services to you.

We have made the essential cybersecurity services that provide proactive monitoring and attack prevention affordable for every company. When services are properly

planned, you implement only what you need. As your company grows and needs changes, your services scale with you.

Quickly calculate your company's investment right here.

Where You Are Now is the Place to Start

If you are using an outsource IT provider (MSP), you most likely have built a trusted relationship with them over time. We all are most comfortable keeping those valued partnerships undisturbed.

But at some point we need to start a conversation that can at first feel awkward. MSPs are often hesitant to initiate the conversation about security services for several reasons.

One of them is that "assume" word again. MSPs know you are assuming their services extend to cybersecurity. After all, they did say "*We take care of all your IT needs*."

What they didn't say is "*As long as they're the same needs you had years ago. We don't do _____ (fill in the blank)*" How can they tell you they don't provide these new security services without putting your relationship at risk?

This is why a comfortable conversation among valued business partners is so important.

You are the client.

You have an obligation to ensure the technology services your company are receiving meet today's security standards. Your technology partners have to be committed to continually growing.

One way to do this is for you to start the conversation with your technology team.

1

You and your technology team (even if you are the entire technology team) will **clearly understand the services currently provided**. Where are the gaps between your assumptions and the actual services provided?

2

You need an actionable risk assessment. Security decisions are based in part on your tolerance for and assumption of risk. Each company is different so you need reliable information to guide your risk decisions.

3

You and your technology team will create a collaborative framework for identifying, planning, and implementing a cybersecurity solution that is right for your company right now.

4

Security is not a one and done project. It is an ongoing, continually changing commitment. You will identify what essential services and skills are lacking in your technology framework. How will you fill those gaps?

Questions to Start the Conversation

These suggested questions are not all-inclusive. They will simply help you start the conversation comfortably.

As your conversation moves along, new questions will arise. By all means, ask them!

Take notes. Right now you're in listening and learning mode.

Let's get started!

One point to be aware of before you dive in –

When you are discussing this with a managed services provider, this can be an uncomfortable conversation for them.

The disconnect between the services they are actually providing and your expectations can lead to some awkward moments.

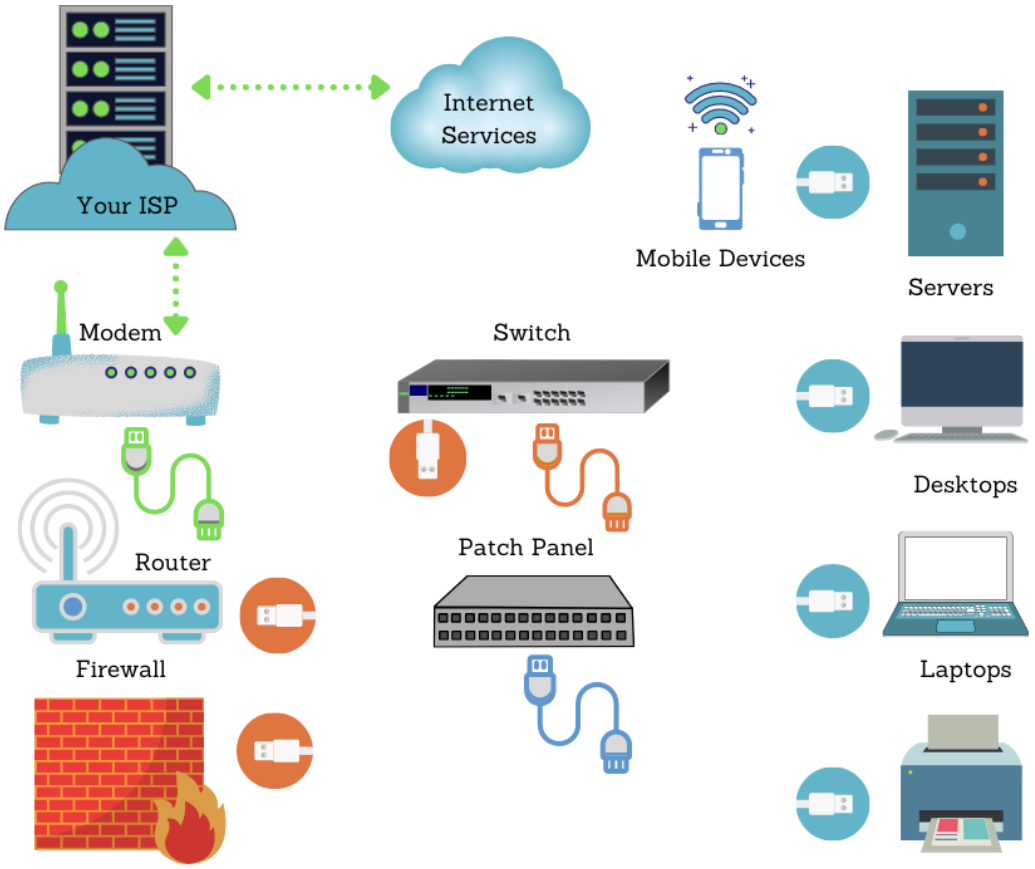
This is the time to simply make notes and continue the conversation. You'll make the right decision after you have more information.

1

You: Let's start by reviewing the services you currently provide to us. Do these include all things related to cybersecurity?

Listen for: Traditional managed service providers will emphasize server, desktop, and laptop updates, anti-virus software, firewalls, and server backups. While these are all important for your day-to-day operations, they are not cybersecurity services.

For your reference: These are components of a typical business network. If all of your applications and data are in the cloud, then you might not have an internal server.



2

You: Will you explain what cybersecurity includes?

Listen for: If the short answer to question 1 is "yes", ask them to explain what that includes. You want to hear phrases like proactive endpoint security, SOC monitoring, content filtering, proactive monitoring, intrusion detection.

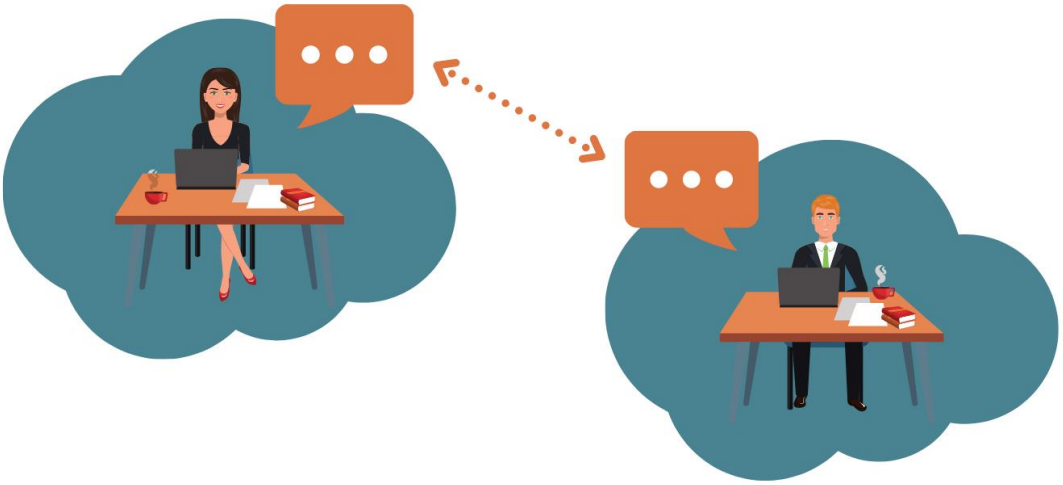
If they say firewall, backups, and antivirus software, then they are not providing the essential proactive security services you need today. These are still important, but they aren't adequate for your company.

If the answer to question 1 is "no", then it's time to add the right cybersecurity skills to your team. We'll cover that at the end of this ebook.

For your reference: The good news is you don't need to suddenly become a technology guru. We've included a short introduction to some of the key concepts that will clarify these baffling technology concepts.

Let's start with the differences between traditional antivirus and the advanced proactive security services companies are adopting today.

What's the Difference Between Legacy Antivirus and Advanced Endpoint Security



Legacy Antivirus

- Users manage the antivirus software on their desktop or laptop
- No centralized control over key update and protection settings
- Scans for known malware from a definition database
- Scans files and processes on the device
- Little protection against modern cyber attacks
- Scans for unknown malware using the heuristic (maybe, trial and error, probable) method
- Updates with new malware definitions done on a schedule
- Lag between new malware definition creation and update increases risk of harm

(c) Quest Technology Group, LLC

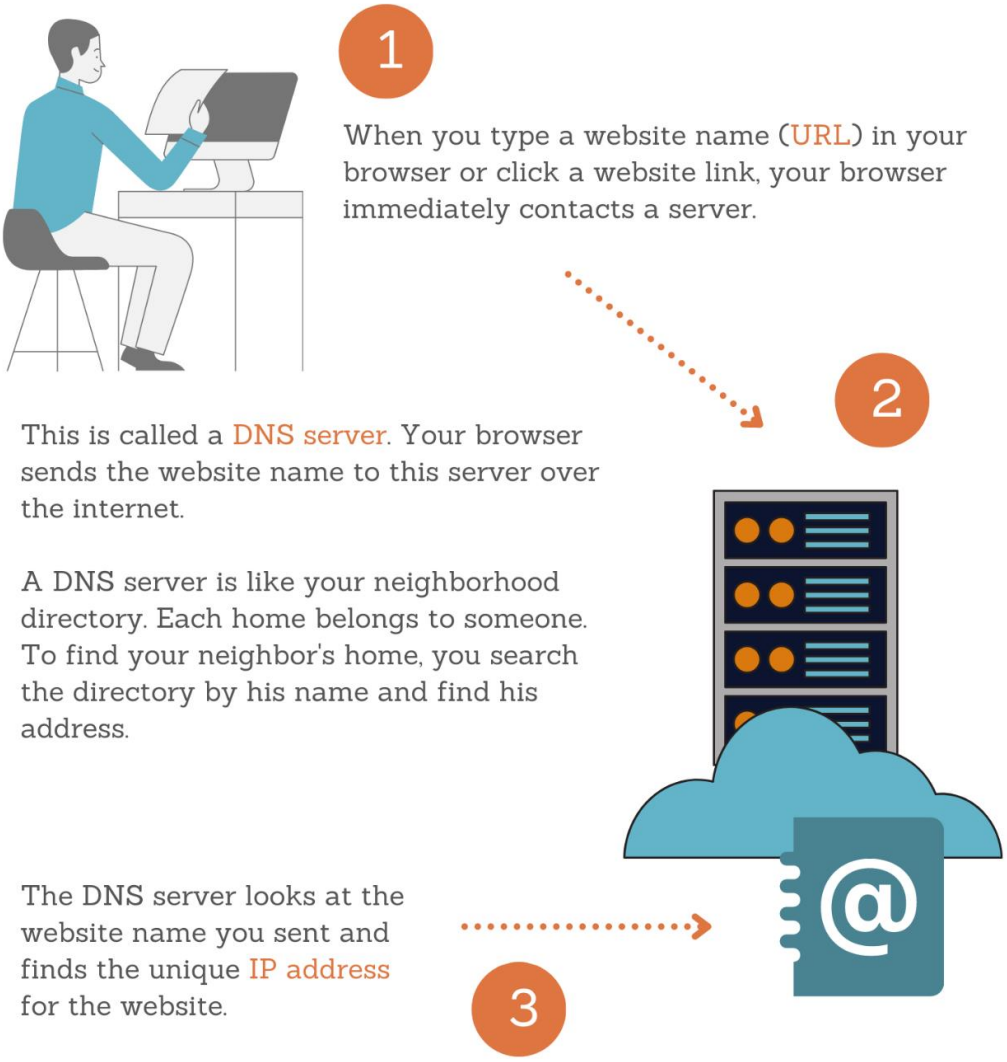
Advanced Endpoint Security

- Users cannot control the antivirus on their desktop or laptop
- 24/7/365 centralized control over essential protection settings on all devices
- Scans continuously for both known and potential malware
- Delivers new malware updates immediately
- Scans the entire device including files, processes, in-memory executables, services, downloads, USB devices, email, and attachments
- Continuously learning and protecting based on user and device behavior
- Predicts and blocks potential threats based on variants of known malware
- Provides partial and full rollback to a healthy state

(c) Quest Technology Group, LLC

You have probably heard about web content filtering if you haven't already implemented it in your company. If you have wondered how it works, here is a quick overview.

DNS Content Filtering Explained



What is an IP address? It is a unique number assigned to a device on the internet or a local network. It allows other devices to find and connect with it on the internet.

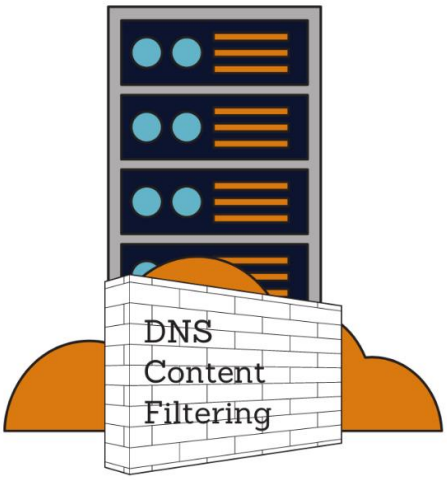
Example: You entered https://www.gohere.com. The DNS server finds this name with an IP address of 199.250.45.2. Now we know which server on the internet has (hosts) gohere.com.

If the IP address isn't found, then your browser displays a message that the website could not be found.

4

Before you can see the website's content in your browser, we need to learn more about this website. This is known as DNS content (or web) filtering.

A request to check this website is sent from the DNS server to a DNS content filtering server.



The DNS content filter server goes through a series of checks:

- Is this website on the list of known potential risk sites?
- Is it a website your company allows?
- Are you allowed to visit this site?
- Does the site contain content that is on the list of blocked categories?
- What rules has your company defined to manage website access?

When the DNS content filtering check **approves** your website, the content filtering server sends the IP address for your website to your browser.

The website is displayed on your browser.

If the website **does not pass** all the tests, then your browser displays a message that the website is not allowed.

The entire trip has been completed in a matter of milliseconds!

3

You: If we have an attempted breach, how will we know?

Listen for: Proactive monitoring services identify and stop attacks before they happen. In most cases, you will never know that an attempt occurred. Your service provider should deliver a regular snapshot of breach attempts to you simply to make you aware of the work being done in the background on your behalf.

4

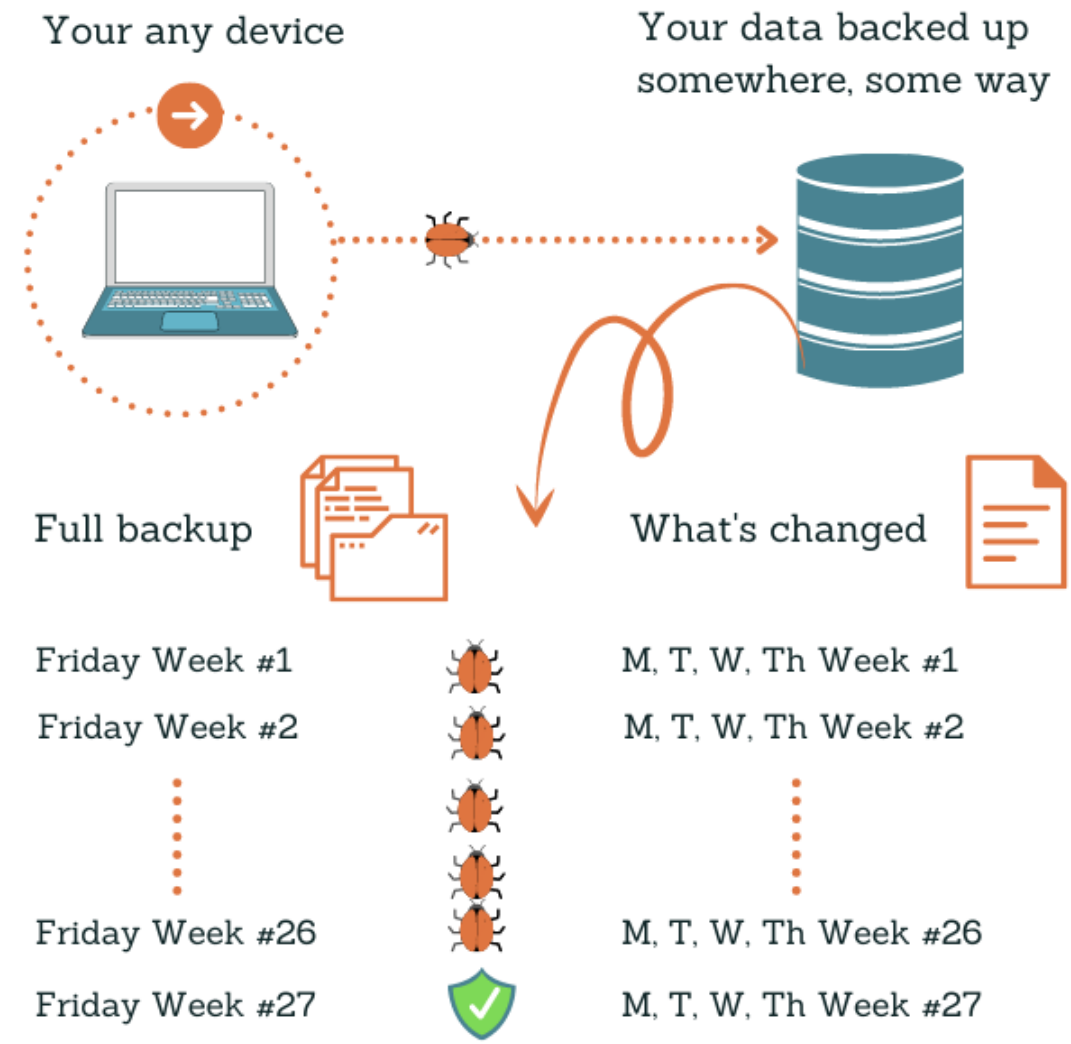
You: If we have an actual breach, what will you do to help us recover?

Listen for: Your service provider should have helped your company prepare a cyber attack action plan. Depending on your business and regulatory / compliance requirements, an appropriate response plan will be your reference.

If they say they will help you restore from backup, you should ask them how they will ensure the integrity of the backup.

Malware, the source of many breaches, often lives quietly on your network or device for many months before coming to life. This means that same piece of malware might be included in your backups. A restore requires caution.

For your reference: Imagine that a piece of malware has found its way into your network. It exists undetected and is included in every backup. It's easy to see how restoring from a backup without carefully inspected it can lead to unpleasant results.



5

You: If we have a loss of company or client data, what will you do to help us take the proper actions?

Listen for: Notifying clients and customers about a data breach should be part of your cyber attack response plan. In fact, there are legal obligations that you need to be aware of.

It's important to remember that your clients' data can have significant value to their competitors as well. Hackers know this and will quickly exploit this stolen data.

Data loss doesn't end with your internal data. The impacts expand quickly.

6

You: Do you provide us with proactive endpoint security?

Listen for: Proactive endpoint security is a fancy phrase for next generation antivirus. Take a minute and go back to question 2 for a snapshot of the differences.

7

You: Do we have 24/7/365 proactive monitoring and attack prevention through a security operations center (SOC)?

Listen for: Security operations centers operate globally 24/7/365. They are staffed by highly skilled cybersecurity specialists who continuously use the latest tools, techniques, and intelligence to watch for and prevent cyber attacks.

The traditional managed service provider does not perform this sophisticated level of cybersecurity monitoring. He or she will provide these services to you through partnerships with SOC providers.

If your provider says they are providing SOC services, ask them for the name of the company they are partnering with.

_____

_____

_____

_____

_____

8

You: We have cyber insurance. How does cyber insurance protect us?

Listen for: Cyber liability insurance is not proactive prevention. Insurance might offer some monetary relief after you have suffered damages, but it cannot prevent an attack.

In fact, insurance companies will review your documented cybersecurity policies and practices to determine how proactive your company is in preventing attacks.

Incorrect answers on your cyber insurance application may be grounds for declining coverage for your claim. Make sure that you have thoroughly documented your systems, policies, and procedures to support your application answers. Teamwork with your IT folks and your carrier is key.

Having cyber coverage does not guarantee reimbursement for losses. The burden to take proactive protection steps along with a written, actively managed cyber defense plan are essential.

9

You: What security credentials does your IT team have?

Listen for: Cybersecurity expertise goes beyond the traditional network administration and support skills provided by most managed service providers. Cybersecurity specialists have the current, hands-on skills to proactively address security incidents, not just how to identify them.

Certifications that benefit your company include Network +, Security +, GPEN, CPT, CISO, and CISSP.

10

You: Do your employees who support us attend cybersecurity education and training courses?

Listen for: A provider who encourages continuous learning for its staff gets a big thumbs-up. Managed service providers realize that the traditional services they delivered are no longer enough. They are committed to refreshing their company and the value they deliver to clients like you to remain relevant.

These service providers are called **Managed Security Service Providers (MSSPs)** instead of Managed Service Providers (MSPs).

Managed service providers who do not promote active learning are comfortable doing what they've always done. This does not serve your company's best interests. Time to reconsider the relationship.

11

You: How often are network assessments, dark web scans, and vulnerability scans performed on our network?

Listen for: Regular network assessments, dark web scans, and vulnerability scans detect weaknesses in your network. Dark web scans should be run monthly. Once an email address has landed on the dark web, you need to respond immediately to prevent further compromises.

Vulnerability scans should be run at least quarterly. Depending on your company's unique needs, scans might need to be done as often as weekly or monthly.

If scans are not being performed on a regular schedule, then you should ask why not. Your typical MSP does not provide this service. These scans are done by experienced cybersecurity specialists.

12 **You:** Do we have a web or content filtering solution implemented?

Listen for: Content filtering is not a core service that managed service providers typically offer, and they simply might not discuss it with you.

Web content filtering blocks access to sites that are offensive, dangerous, or inappropriate. Malware can find its way into your network through these websites. Inappropriate sites also leave your company exposed to hostile workplace claims.

13 **You:** How are we protected against data breaches when our employees work from home or remotely?

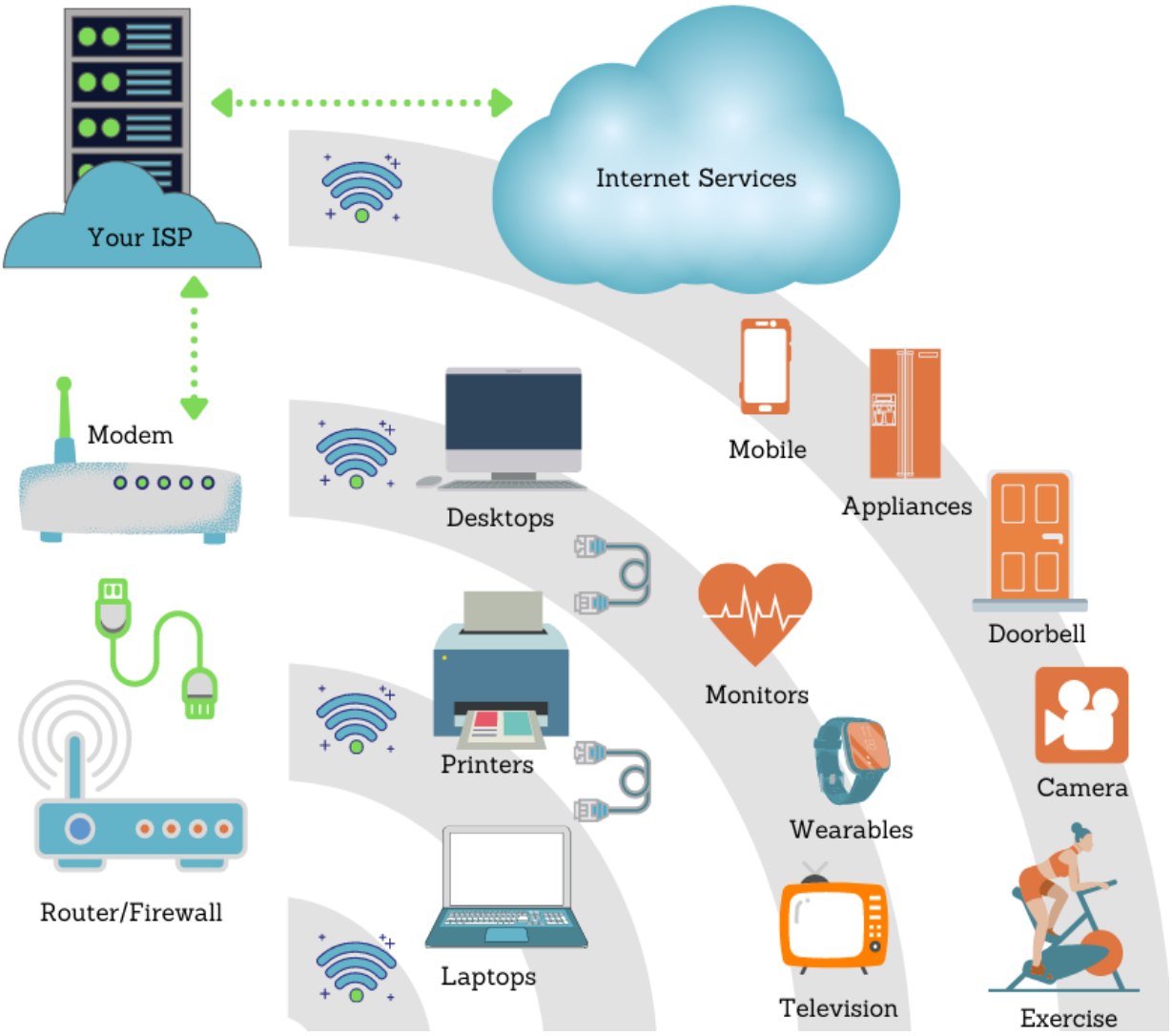
Listen for: Remote and work from home are a way of life for most of us today. Whether it's from home, a remote job site, or a local café, your employees have access to a tremendous amount of company data wherever they are. This creates additional opportunities for hackers to exploit weaknesses in your network and individual devices.

Since this is a broad topic and remote work policies vary by company, we recommend you and your provider have a detailed discussion about best solutions for your company. Ask them to explain in plain English how all remote access points are being protected. Better yet, ask them to draw the picture of your network.

It is not unusual for a managed service provider to say they do not support home networks (a potential risk) or out of office work.

How is a Home Network Different Than a Business Network?

When you look at the home network below, one thing quickly stands out. Your home network is more than just your household using the internet and some applications. All your smart devices have quietly joined your network. They are also using your wifi to continually send and receive information over the internet.



You can learn more about how data travels and how it is stored on cloud servers here. Companies have safeguards in place that the typical home network doesn't have. Here are a few differences.

Business Network	Home Network
The company's IT team manages internet traffic using strict firewall rules.	Your router/firewall combo has no predefined rules to manage internet traffic.
The company's IT team manages router and firewall passwords.	Home wifi routers and devices often use the factory default passwords. This makes unauthorized access to your home network too easy.
The company's IT team manages who has access to the network. This protects both the company's and clients' data.	Anyone with access to your home network can access everything on every device.
Companies have policies on what software and applications can be downloaded, installed, and accessed by each user and device.	Installing, downloading, and accessing any software and app is risky.

14

You: Do you perform regular vulnerability scans on your own network?

Listen for: Best security practices should be adopted by and continuously practiced by your provider. It's like asking your dentist how often she flosses and being told "when I remember to do it". Ugh. Not a comforting reply, is it?

15

You: What are your internal security policies and protocols?

Listen for: How does your provider protect its own internal network? Your provider should have implemented the advanced security and proactive policies you expect for your own network.

16

You: Where is the data you have about our company stored?

Listen for: Your provider likely has information about your company's network, passwords, and other critical pieces of data that must be protected.

Ask them what data they have and where it is stored. If they use third-party services such as cloud storage or web applications, what are they?

Do they use a secure online password manager such as LastPass?

If you terminate services with them, what happens to this data?

17 **You:** Who has access to your company's data?

Listen for: Your company data is valuable, and your provider has access to a lot of it. Every employee who supports your organization has some level of network and device access.

How does your provider manage this access? What happens when an employee leaves their company?

_____

_____

_____

_____

_____

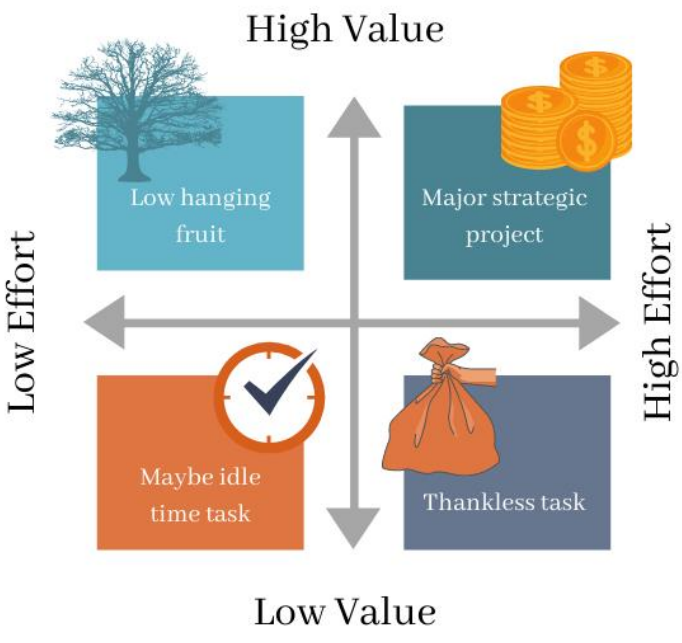
18 **You:** What tools are used to access your network?

Listen for: All managed service providers have remote access to their clients' networks for support and maintenance. There are widely-accepted tools that provide secure access. Ask them what tools they use. If they tell you remote desktop, then you should be concerned.

What is a Cybersecurity Risk Assessment?

A cybersecurity risk assessment identifies, analyzes, and evaluates risks for a cyber attack, breach, or internal weakness. This includes exploring your company's assets that could be affected by an attack such as networks, hardware, desktops, laptops, company data, and customer data.

As the likelihood and frequency of attacks occurs, understanding your company's risk is critical. Each company is unique, and the factors that define risk will vary.



(c) Quest Technology Group LLC

With our clients, we recommend four assessments. Here is a quick overview of each.

1. We start with a **network discovery**.

   This identifies the servers, desktops, laptops, on the network. For each of these the discovery tools report valuable information about the software and users for these devices.

   From this discovery, we create an action plan. Since each client is different, we work closely with them to identify and implement the right steps.

2. A lot of the information collected in the network discovery is used for the **vulnerability assessment**.

   This discovery is done by a security specialist with software designed especially for this. It identifies additional weaknesses and vulnerabilities.

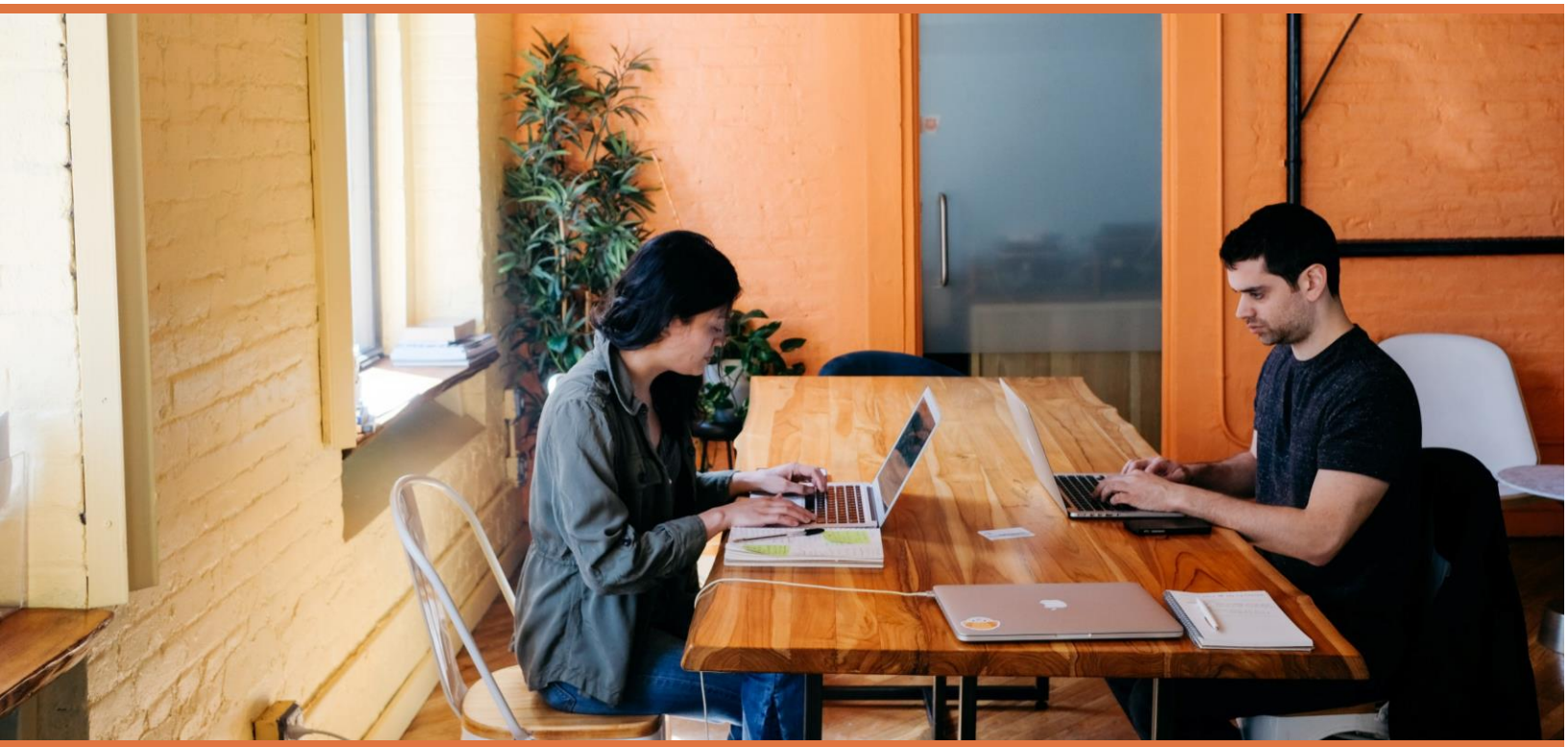
3. A **physical assessment** is a detailed survey of the company's premises.

   While network security is critical, physical security of your facility is just as important. This is often overlooked and offers unexpected opportunities for data theft.

4. A **pentest** uses software that mimics an actual attack.

   A security specialist applies all of the known exploits hackers use on your internal network.

What to Do Next



Does all of this sound complicated and expensive? We understand how overwhelming this can feel.

If you're like most of us, this conversation has simply created more questions. That's exactly where you should be. You've just scratched the surface. You are ready to continue adding to your knowledge store.

Your role as a company leader is not to become a technology expert. Instead you need to have the knowledge to make informed, confident decisions for your company's long-term health.

We're Ready to Help You Get Started

Quest Technology Group is committed to helping companies like yours make informed technology and business decisions that best serve them and their clients. We believe this starts with knowledge.

A lot of knowledge.

Technology and business go hand in hand but knowing how they work together can be frustrating and time-consuming. As your technology partner, we'll connect the baffling dots with you.