CONCENSUS TECHNOLOGIES

YOUR GUIDE TO CYBERSECURITY

CT | CONCENSUS TECHNOLOGIES

TECHNOLOGY SOLUTIONS FOR A NEW NORMAL

The good news is that there are methods, processes, technologies, and policies that can build the secure environment you need to protect your business.

Specifically, using a multi-security, multi-layer approach can protect you from these common types of attacks, among others:

- Spam
- Viruses
- Malware/Ransomware
- Phishing/Spear Phishing Emails
- Hacking
- Data Loss
- Denial of Service (DoS) attacks

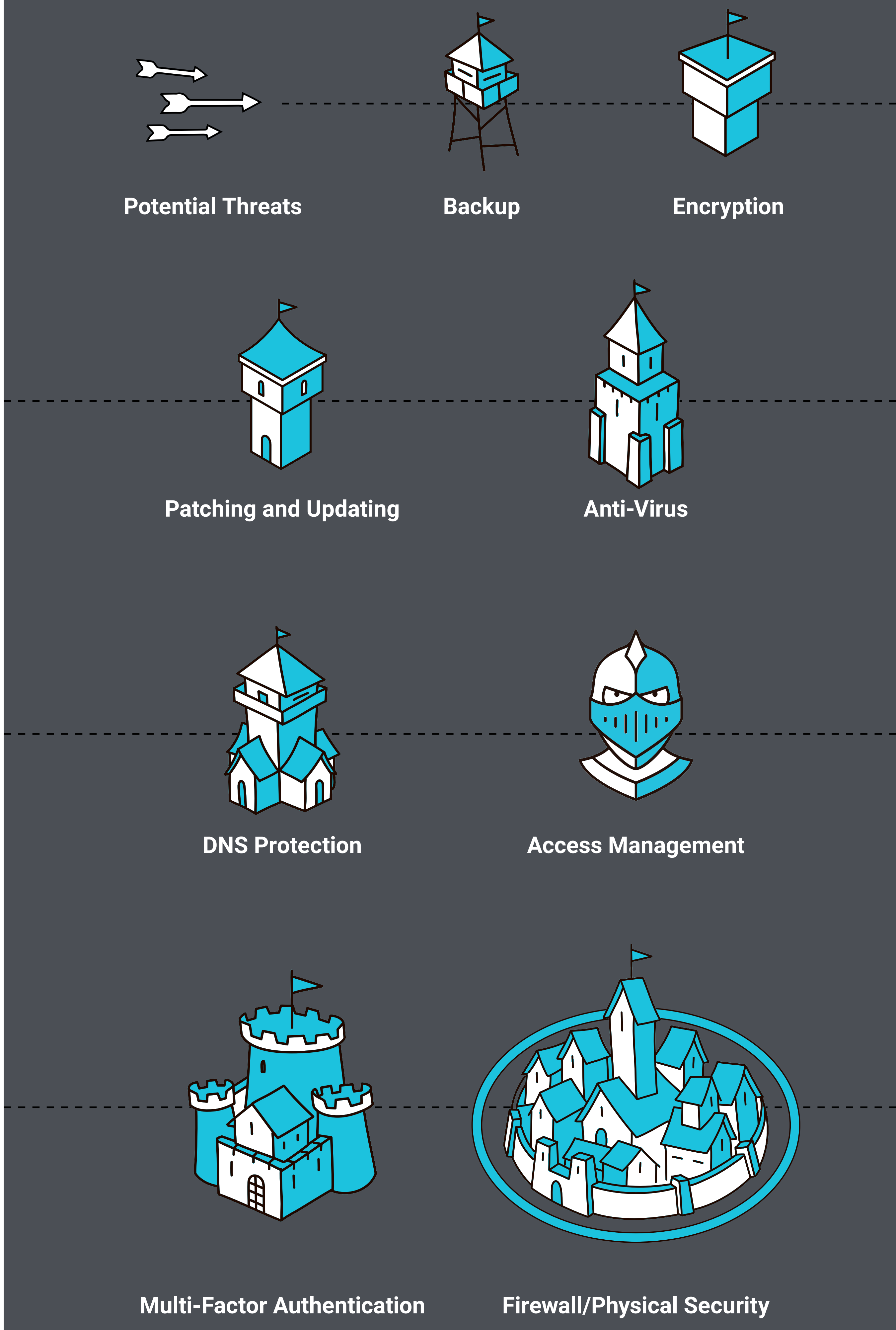
Cybersecurity technologies are also preventing attacks from a new form of cybersecurity threats known as the "Dark Web". The dark web is an underground and unregulated part of the internet that is home to black markets and underground or criminal activity. It is a network of hidden URLs that are generally not found via search engines or other types of websites.

Through today's cybersecurity experts, you have access to the necessary security measures and guidance to keep you, your information, and your business safe while giving you focus and peace of mind.

The following guide provides you with information on the various avenues of cybersecurity. It begins with means to assess your systems, then discusses the items for your consideration on hardware, software, processes, employee concerns, corporate policies and what to do moving forward.

NONE SHALL PASS!

Designing your cybersecurity strategy starts with identifying the digital assets that need protection, just like a medieval castle was designed to protect the gold in the keep. Castles didn't rely on just one strategy for protection. They used knights, guards, castle walls, the landscape, and a moat. You, too, should layer your cybersecurity with multiple defenses.



TYPES OF ASSESSMENT TOOLS

Vulnerability Scans

Knowing where your online cybersecurity vulnerabilities may lie, starts with a comprehensive vulnerability scan. Network vulnerability scanning is an in-depth review that will give you insights and information on every connected device on your network and take an inventory of all of your systems, including the operating system, patches, installed software, hardware, anti-virus and firewalls, and more.

Sophisticated scanning software provides reports that:

- ✓ **Reviews all systems and connections**
- ✓ **Organizes the number of threats**
- ✓ **Identifies where the threats exist**
- ✓ **Classifies the type of risks**
- ✓ **Offers the appropriate solution**

Your Overall Security Assessment plan should consider the following:

- ✓ **Frequency of running vulnerability scans to protect your networks, systems, data, and users against harmful cybersecurity threats and attacks.**
- ✓ **Performing the vulnerability scans during regular business hours to collect as much data from as many systems as possible.**
- ✓ **Pairing your vulnerability scans with annual penetration tests to ensure your systems are comprehensively secured.**

Penetration Scans

Penetration scans, also known as “Pen scans” differ from vulnerability scans. Whereas vulnerability scanning focuses on device-level weaknesses for prevention, a penetration scan is an active attempt to gain access to a system through a known weakness or by manipulating an end-user. Typically, a penetration test simulates a cyberattack such as hacking or phishing to evaluate the security of the system.

Penetration testing should be minimally performed on an annual basis, best practices suggest vulnerability scanning on a once-a-month or quarterly basis, at the very least. However, both are requirements for a comprehensive approach to cybersecurity, and the two efforts work in tandem.

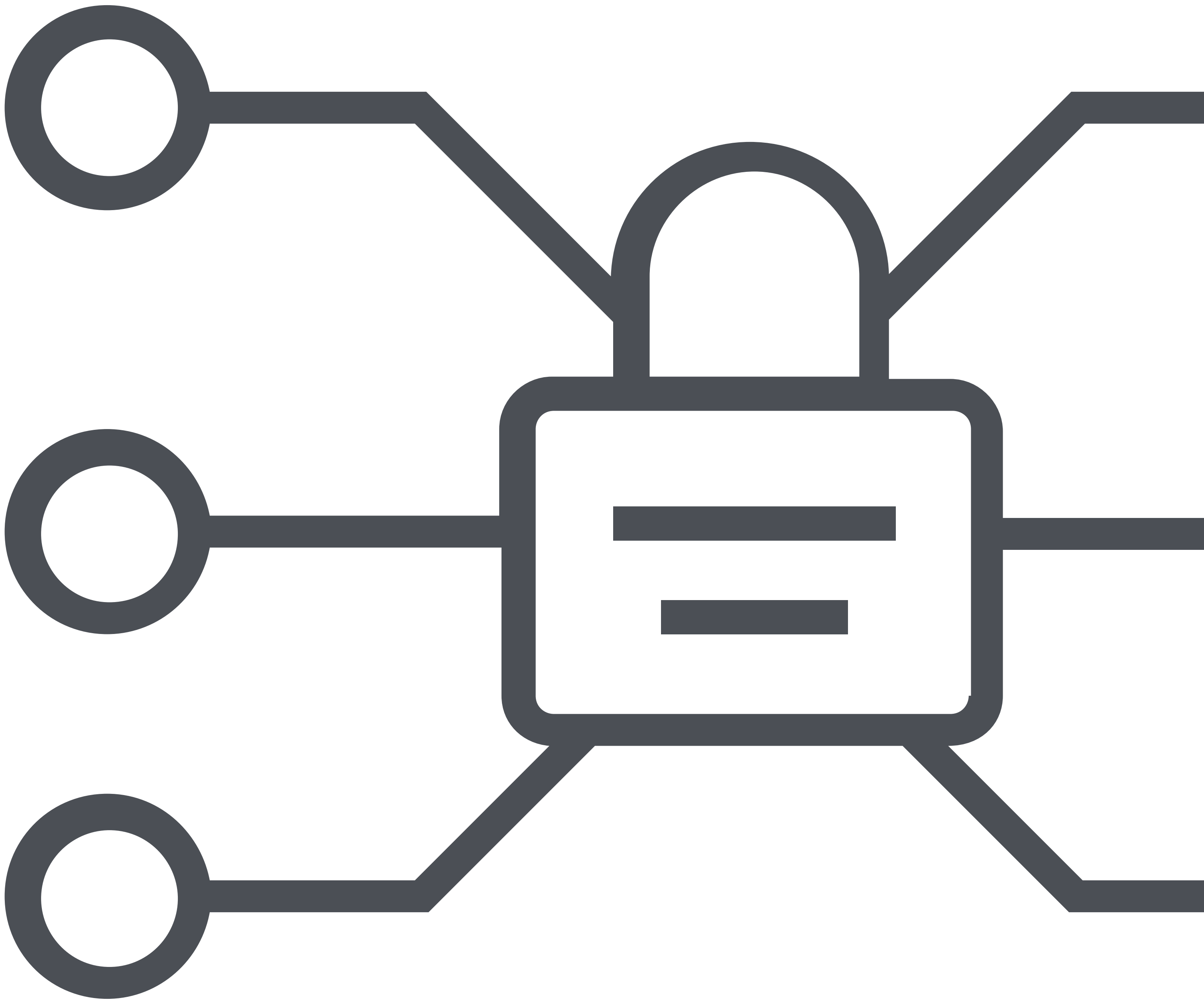
Log Management

Most IT systems can generate log files. Effective log management happens when the method is combined with software solutions that automatically turn off ports in a network firewall or immediately lock-down an insecure account.

Logs also provide vital insights for investigating an organizational security breach or a targeted cyberattack. Best of all, when logs are analyzed in real-time or near real-time, this helps prevent a cybersecurity attack.

Automated Log Management software reads the data in real-time and provides statistics and alerts based on the information. This thorough, real-time approach is also referred to as Security Information and Event Management (SIEM). The automated approach makes it faster and easier for your organization or IT team to take swift action if and when a security threat occurs. Once you’ve implemented your SIEM solution, start the process by analyzing the firewalls, systems, and application logs.

MULTI-LAYER SECURITY MEASURES



Physical IT Security

The physical aspect of cybersecurity is often neglected since so many dangers lurk out in cyberspace. But a critical aspect of cybersecurity begins with **making sure your on-premise servers, networking equipment and other devices are physically safe from malicious individuals.**

Best practices for physical IT security include:

- ✓ Lock systems in a physical room and limit access. Have people sign into the room for auditing measures of who is in and has accessed the room.
- ✓ Lock down server and desktop USB ports via physical locks and security software to prevent the installation of malware or theft through the USB port.
- ✓ Monitor the area with high security cameras
- ✓ Use remote access cards for example iDrac by Dell or ILO by HP
- ✓ Adequate power and cooling
- ✓ Password Protect System Bios
- ✓ Do not place servers under a sprinkler
- ✓ Lock the Case
- ✓ Use a Locked Rack and secure the key or combination

Other physical IT security considerations include the building safety, adequate staffing and visitors connecting through internal network ports in common areas.

Modern Workplace Management Security Measures

Modern Workplace Management covers all devices, also known as Endpoints, to prevent or stop attacks. It incorporates the policies, technologies, and implementation processes needed for early detection and overall security of your network. Management of Workplace Endpoints includes such items as:

- ✓ Upgrading OS to Microsoft Windows 10 using the Professional or Enterprise version
- ✓ Device Patching and Upgrading
- ✓ Remote Monitoring and Management tools
- ✓ EDR (Endpoint Detection and Response)
- ✓ Individual Device Backup
- ✓ Device Encryption (Bitlocker/Windows; FileVault/Mac)
- ✓ Updates to company IT policies
- ✓ Procedures for Implementations

Email Security through Third-Party and DNS protection

Email is the most vulnerable application and the most prevalent means for a cybercriminal attack. Increased email security can help protect you against malicious messages, data loss, and help you meet compliance requirements.

A trusted, third-party advanced security layer for your email system is a vital element of effective multi-layer security. A few features include:

- ✓ Advanced Threat Protection (Spam, Viruses, Malware) - Scanning email attachments in the most commonly used file formats and compares them against known threats.
- ✓ Anti-Phishing - When an email comes in and looks like a valid email, it may not be as it appears. Anti-Phishing algorithms help to detect and flag fraudulent emails by reviewing emails with anti-fraud intelligence, checking to see if the sender is a valid user and checking links to ensure they are not directing you to a known malicious site.
- ✓ Data Loss Prevention - When private information is available to employees, it is important to be able to detect if it is being sent outside the organization. A policy-based screening of this information can prevent the emails from being sent.
- ✓ Secure Emails When private information needs to be sent securely to external users, secure emails send the information via an invitation to a website. From here, the intended recipients can verify their identities and download the contents.
- ✓ Message Archiving - Provides a complete backup of all employee internal and external messages

Secure DNS Protection

Secure (Domain Name Systems) DNS protection as part of a multi-layer strategy that comes into play when your email spam/anti-virus solution does not catch a malicious email. If the end user receiving the email would click a link to a malicious site that is known to the secure DNS protection service, the service will block access to that site preventing the user from even seeing the malicious website.

DNS tracks all the sites and their locations, both good and bad. DNS solutions should be cloud-based since it is updated every day to block as many malicious sites as possible. A strong secure DNS protection solution will also provide a web filter to block sites by category (gambling, drugs, etc). In some cases, reporting on end users web browsing history is required for compliance. Many of the DNS protection solutions also provide detailed history reports by device and user.

Firewall Protection

Firewalls proactively:

- Identify and prevent incoming viruses
- Recognizes and blocks when someone is actively scanning your network for access vulnerabilities
- Allows external communication and secure data exchanges
- Contains Intrusion Prevention System (IPS) features

Due to the amount of cybercrime, modern-day network security requires next-generation firewalls. Next-generation firewalls are also capable of blocking internal users from spreading a virus internally or infecting machines outside of your network, whether intentionally or accidentally. Considerations to help you determine your firewall solution:

- Number of users you need to support since firewalls are rated for the number of users/devices.
- Understand your internet speed, connections, and capabilities.
- Consider if you have multiple sites and whether they will be connected via a private network or through the internet. Specifically, be aware if you will be connecting to a public cloud such as Amazon AWS or Microsoft Azure. Also be aware if your users will require VPN access
- Which additional layers of security that may or may not be in place, for example, anti-virus, DNS protection, web filters, and others, in cooperation with the firewall.

Multi-Factor Authentication

Multi-Factor Authentication (MFA) is a security system that verifies a user's identity by requiring multiple credentials. For example, these credentials might include a code that is sent to the user's smartphone or require answers to a set of security questions, or they may be more intricate security measures, such as fingerprint scans, retina scans, or facial recognition. MFA creates multiple layers of security to help increase the certainty and confidence that the user requesting access is who they claim to be.

MFA solutions can incorporate additional factors by considering the context and behavior of a user when authenticating. For example:

- Where a user is trying to obtain access (office/home/other)
- When or what time of day a user is trying to access (late at night/typical workday hours)
- What device is being used (smartphone/tablet/laptop)
- What kind of network is being accessed (private or public)

With MFA in place, a cybercriminal or hacker may steal one piece of a user's credentials but can be thwarted by having to steal additional security measures, as well.

EMPOWERING EMPLOYEES FOR SECURITY DEFENSE

Creating Security Awareness

Cybersecurity is everyone’s responsibility. Unfortunately, for businesses and organizations of all sizes, users are typically the weakest link when it comes to phishing attacks and scams. Therefore, you can’t afford to wait until a cybersecurity breach or security event occurs to take action on awareness, training, and comprehensive protocols.

Organizations can benefit from purchasing a subscription to a Security Awareness Training (SAT) service. This service provides a series of online modules and quizzes to train and test users across your organization. Specifically, end-users take modules that educate them on passwords, email security, website security, physical security and on their awareness across the essential areas of cybersecurity. Employees can also be tested to identify a fake or phishing email, and be evaluated to see if they input passwords, private data, or have a tendency to click on dubious links.

The benefits of Security Awareness Training are two-fold: First, it safeguards the business with a preemptive layer of protection. Second, it increases your eligibility for cyber insurance regarding the qualification question: “Do you provide training to your employees?”

Cyber Hygiene also known as IT Cleanliness

Anyone can fall victim to fraud or cyberattacks. It is much easier for a cybercriminal to trick you into clicking a link than hack into a high-tech firewall. So, by practicing consistent methods of Cyber Hygiene, IT security and online safety will improve.

Here are a few ways to practice Cyber Hygiene:

- Use a password manager and create long random passwords.
- Use a PIN for account recovery questions before or after your answer. For example, if your security question is “What’s your favorite color,” your answer could be BLUE7748.
- Keep all machines, applications, and antivirus solutions up do date.
- Keep a running inventory of all of your network’s hardware and software and install GPS tracking software.
- Backup important data in more than one place, such as on disk and in the cloud.
- Create an incident response plan covering what to during and after a hack or security breach.
- Discourage the use of public Wi-Fi by ensuring access to your private Wi-Fi-network.

Company IT Policies

No matter what you decide your policy to be, you must make sure it is clearly stated and documented in your Employee Handbook and Acceptable Use Policy. Review your employee handbook with regards to IT procedures and devices and verify that you have adequate protection in place. The following are some suggested items to review with a trusted advisor:

- Internet browsing policies. These should be able to be enforced by individual, group, device or network. DNS protection can block sites such as adult entertainment, gambling, social media, and streaming services via policy.
- Backup, archiving (or data retention) policy
- Workplace policies for the regulation of Endpoint devices
- Rules governing using personal devices for work, also known as Bring_Your_Own_Device, or BYOD. Specifically state the manner personal devices are to be used and if they can be used to access the network
- Include policies referring to the Implications of hands-free, phone calls, and texting functions while driving
- State laws on personal cell phone use and general liability, especially when distracted by business calls or texts while driving
- IT policy changes for working remotely considering the new wave of security issues for home-based work and offices

CREATING A PLAN

A Cybersecurity Response Plan

If your systems are hacked, inform your internal teams and any third parties or vendors.

Most businesses or organizations will experience a cybersecurity incident. Regardless of the size or scope of the incident itself, your organization needs a comprehensive cybersecurity incident response plan. This plan contains an established set of pre-determined rules, urgent tasks and steps to take if you have confirmed that your organization has experienced a security breach or cybersecurity incident.

As part of the response plan, you should already have in place before a breach occurs:

- Privacy Policy regarding client data
- Security Policy
- Social Media Policy
- Security Control Measures
- Backup/Recovery Technology
- Cybersecurity Insurance

Then the response plan should include the manner to isolate the incident, inform necessary third-parties such as insurance, banks, authorities, and the manner to inform clients if their data has been compromised.

Backup and Recovery Processes and Plans

Cybersecurity breaches teach us that we need reliable data backup. Just as important is enabling these backups to restore company data quickly.

Your backup plan needs to be comprehensive in order to recover from a data or system loss and all concerned should follow corporate policies regarding backup. Any solution that you implement should seamlessly backup all of your data whether it is on premise or in the cloud.

If you have local systems, have both an on-premise backup for faster recovery of your systems as well as an offsite copy. When you are evaluating your backup plans you need to ensure the following:

- Comprehensiveness (does it cover from local disk to my software as a service?)
- Recoverability (how quickly can I get it back?)
- Performance (How long will it take to get that system back up and running?)
- Reliability (Can we prove or test our backups work?),
- Affordability, and scalability (will i quickly outgrow my investment?).

Cyber Insurance Coverage

Cyber insurance works just as any insurance and in the case of a breach will provide coverage to help assess and cover the costs. Cyber insurance companies may also provide access to cyber breach coaches and other service providers to help aid recovery efforts.

Most cyber insurance covers:

- Data loss and recovery
- Business interruption or revenue loss
- Loss of transferred funds
- Computer fraud
- Cyber extortion

The insurance company will usually require proof of compliance with the insurance agreement, comprehensive cybersecurity policies across your organization, ongoing employee security training, and auditing of security technologies all being maintained and updated before granting coverage.

CYBERSECURITY:

PARTNER WITH A MANAGED IT SERVICES PROVIDER

Cybersecurity, is of course, a top priority.

Even if you already have an IT department, you (and they) need access to the experience, capabilities, and guidance of trusted cybersecurity experts through a managed IT service provider.

Choosing the correct managed IT service provider is imperative to your success and security.

At Concensus, our experienced and expert cybersecurity team is here to protect, support and guide your defenses against the world of cyberattacks, cybercrimes and cybercriminals.

In addition to the items listed throughout this guide on cybersecurity, Concensus can deliver peace of mind by:

- Securing your networks, connections, devices, and applications
- Identifying threats and vulnerabilities and manages their fixes
- Implementing services and technologies to prevent attacks before they happen
- Supporting both your on-premise and work-from-home employees
- Advising on policies
- Advising on cyber insurance
- Adhering to compliance regulations, for example, those that HIPAA and SOX, and cyber insurance carrier
- Being a backup and recovery solution partner
- Continually monitoring, updating, and providing the latest in cybersecurity protection
- Implementing the cybersecurity measures to shelter your business and information from the new threats of an ever growing and evolving world of cybercrime

At Consensus, we are the team of cybersecurity experts you need and need now, in this turbulent world of cybercrime. Contact us today to begin receiving the protection you require and deserve at www.concensus.com/healthcheck.

CONCENSUS
TECHNOLOGIES

51 DUTILH ROAD, SUITE 140
CRANBERRY TOWNSHIP, PA 16066