advantage
TECHNOLOGY

EVERYTHING YOU NEED TO KNOW ABOUT

CYBERSECURITY

BUT WERE AFRAID TO ASK

advantage

TECHNOLOGY

If you spend more on coffee than on IT security, you will be hacked.”

– Richard A. Clarke, National Coordinator for Security, Infrastructure Protection and Counter-terrorism for the United States

EVERYTHING?

CONGRATULATIONS! YOU NOW HAVE EVERYTHING YOU NEED TO KNOW ABOUT CYBERSECURITY RIGHT AT YOUR FINGERTIPS. I BET YOU THINK THAT'S A PRETTY BOLD PROMISE FROM SUCH A SHORT BOOK, BUT IT'S TRUE!

To be clear, this manual doesn't promise to provide you with everything there IS to know about cybersecurity. But if you're a business owner, executive, have a leadership role in an organization or are just looking to keep yourself safe online, this manual will provide you with everything you NEED to know.

Even if you're an IT manager, you'll find some helpful information in here. And, if nothing else, it'll give you something you can show your users to help them understand their role in cybersecurity.

> *"Cybersecurity is a shared responsibility, and it boils down to this: in cybersecurity, the more systems we secure, the more secure we all are.*
>
> - JEH JOHNSON, SECRETARY OF HOMELAND SECURITY

Phone: 866-793-8232
Email: solutions@advantage.tech

CONTENTS

Phone: 866-793-8232
Email: solutions@advantage.tech

CYBERSECURITY QUICK START!

Top 10 Cybersecurity Tips

TOP 10 CYBERSECURITY TIPS

For those of you who are busy and just want to get straight to the point, here are the top 10 cybersecurity tips. Implement these, and you'll be much more secure than you are now. But don't let that lure you into a false sense of security. As soon as you can fit it into your schedule, read the entire book so you can see the whole picture.

1

HAVE THE RIGHT MINDSET

View yourself as a target and be suspicious of every interaction you have on the internet. Every email, every website that asks for personal information and every free app should get a second look.

2

USE UNIQUE PASSWORDS

Make unique passwords by including the name of the website in the password itself. Start with your regular password and then add the website name to the end. This will give you a unique password for every site that is still easy to remember.

3

ENABLE TWO-FACTOR AUTHENTICATION

Enable two-factor authentication for any service that offers it. Rather than just requiring a password, two-factors authentication requires two things; something you have and something you know. For example, accessing an account would require a fingerprint scan (something you have) and a password (something you know).

4

LOCK YOUR DEVICE

Always lock your device with a password, PIN number or biometric scan such as a fingerprint or facial recognition. Your devices contain all the information a cybercriminal would need to steal your identity.

5

NEVER LEAVE YOUR DEVICE

Never leave a device unattended in a public place. A stolen laptop or phone can be a treasure trove of identity information for a skilled cybercriminal and are hot commodities on the black market.

Phone: 866-793-8232
Email: solutions@advantage.tech

TOP 10 CYBERSECURITY TIPS

6

UPDATE YOUR SOFTWARE

Always keep your software up to date. Whether it's your phone, computer or even a program you use frequently, don't brush off security patches. Patch early and often.

7

CALL A FRIEND

If you get an email from a friend or colleague that looks suspicious, call the person and verify that it's actually coming from them. Especially if the email says they are trapped somewhere where they can't receive phone calls.

8

NO PERSONAL INFORMATION VIA EMAIL

Be suspicious of any official-looking email that asks for personal information such as a bank account or Social Security number. No legitimate organizations will ask any personal information in an email, including usernames or password.

9

SECURE YOUR WI-FI

Protect your home or business by securing your network. Make sure your Wi-Fi network is secure, hidden and password protected.

10

DON'T USE PUBLIC WI-FI

Never use public Wi-Fi networks. You have no way of knowing about the security of the network, and cybercriminals often use public Wi-Fi to access unsuspecting victims. Instead, use your own mobile hotspot or personal hotspot on your phone.

Phone: 866-793-8232
Email: solutions@advantage.tech

SHOULD YOU EVEN WORRY?

Or is Cybersecurity just for geeks?

YOU HAVE A LOT TO LOSE IF YOU DON'T TAKE CYBERSECURITY SERIOUSLY. *THE THREAT IS REAL,* IT'S EVER INCREASING AND IT'S BECOMING MORE SOPHISTICATED BY THE HOUR.

A Global Threat

Cybercrime has become a global threat, with companies as large as Sony Pictures and Equifax becoming victims of what most experts agree are state-sponsored attackers. However, **all businesses and individuals** are highly susceptible to attack thanks to modern tactics such as ransomware, pharming, and phishing (more on those later). Increasingly, cyberattacks are originating outside of the United States from a wide range of countries, including China, Germany, Great Britain and Brazil.

Risk to Individuals

Cybercriminals stand to gain a lot with very little risk. By just setting into motion a few simple attacks, cybercriminals stand to reap a treasure-trove of Personally Identifiable Information (PII), financial information or cryptocurrency payments like Bitcoin.

All PII has some value in the criminal underworld. Obviously direct financial information such as bank accounts and credit cards are the most valuable, but PII can be used to open new accounts, create fraudulent immigration documents or even acquire prescription drugs to be sold on the street.

With the advent of ransomware, cybercriminals can infect your system and **hold all your data hostage unless you pay them directly.**

Skilled attackers even can acquire sensitive information to be used for blackmail or to destroy your reputation.

Risk to Business

Businesses face the exact same threats that individuals face with the added layers of **customers, employees and business continuity being at risk.**

A data breach at a business puts every customer's PII at risk. A ransomware attack will grind the business to a halt, and leaked emails can destroy an executive's status. Any of these types of cyberattacks can decimate the business's standing in the community and possibly shut it down for good.

Because of the threat that customers face, many agencies (both governmental and private) have been established to protect consumers. Non-compliance with agency regulations can lead to fines, legal penalties and even litigation.

Phone: 866-793-8232
Email: solutions@advantage.tech

3

UNDERSTANDING THE THREAT

The actors, their tactics and the results.

THE ACTORS

THE BAD ACTORS IN CYBERSPACE COME IN MANY DIFFERENT FORMS AND THERE'S PLENTY OF OVERLAP BETWEEN THE DIFFERENT TYPES. GENERALLY SPEAKING, THESE BAD ACTORS FALL INTO A FEW BROAD CATEGORIES.

Hackers

Skilled computer users that seek to discover flaws in computer systems that allow them access to a part of a system without proper authorization. Hackers generally fall into two categories, white hats and black hats. White hat hackers search for flaws to fix them while black hats search for flaws to exploit them.

Crackers

Specifically a black hat hacker. Crackers' only goal is to exploit computer systems.

Script Kiddies

Unskilled computer users that use code and exploits created by hackers. The simple code most often used by hackers is called "script," and most script kiddies are young and inexperienced; knowing how to execute scripts but not create their own.

Hacktivists

A type of hacker that sees their activity as political activism. The activity can include obnoxious activity such as publishing graffiti on a corporate or governmental website or taking over a social media account. It also can include blatantly illegal activity such as releasing classified information, Distributed Denial of Service Attacks (DDoS) or stealing financial information.

Cybercriminals

These bad actors may or may not be hackers. They might simply use information taken by hackers, or they may develop their own cyberattacks. Their purpose is to acquire and use stolen information or attack users solely for gain.

Phone: 866-793-8232
Email: solutions@advantage.tech

THEIR TACTICS

BAD ACTORS EMPLOYEE MANY TACTICS TO ACCOMPLISH THEIR ENDS. SOMETIMES, THEY USE SOPHISTICATED SOFTWARE AND SOMETIMES, IT'S JUST A CLEVER TRICK. SOME EVEN BUY THEIR TOOLS FROM ONLINE BROKERS. NOT ALL TACTICS ARE ONLINE EITHER; SOME ARE IN THE REAL WORLD. A GOOD UNDERSTANDING OF THEIR TACTICS WILL HELP YOU IDENTIFY THEM.

Malware

Any software intended to damage, disable or take control of a computer system without the owner's consent. Malware comes in a variety of forms, each with a specific use.

VIRUSES

A form of malware that replicates across computer systems by infecting another piece of software. Viruses were most common before the Internet when people would share files via floppy disks or flash drives. The virus would infect the drive. Whenever another computer loaded it, it would infect that computer. Viruses still exist today, but they are more likely spread via fraudulent email, websites that have been corrupted or downloading corrupt software from disreputable websites.

In the past, viruses would do bad things such as delete files or lock a computer. But today, they are typically more of a delivery system for other types of malware.

WORMS

Similar to viruses, worms spread across computer systems, but a worm self-replicates rather than infecting other software. A typical way this happens is when a person gets an infected email and opens an attachment. The worm executes and emails itself to everyone in the contact list, potentially replicating to everyone the person knows. Also, like viruses, worms tend to be more of a delivery system for other forms of malware.

SPYWARE

Running invisibly on your computer, spyware attempts to glean valuable information by capturing everything you type and the types of activity that take place on your computer. Spyware is able to capture password information, record financial transactions or even who you're emailing and what you're discussing.

Phone: 866-793-8232
Email: solutions@advantage.tech

Malware (continued)

TROJAN HORSES

Often delivered by a worm or a program claiming to be something else, a trojan horse gives a hacker total control of your computer. They can watch what you are doing, dig through your system for valuable information, install other malware or hijack your computer and use it as part of their network.

ROOTKITS

A series of software tools that enable an attacker to take control of an operating system at the root level. The root level is the absolute base level where there are no security protections, allowing the attacker to take over the system or install additional malware.

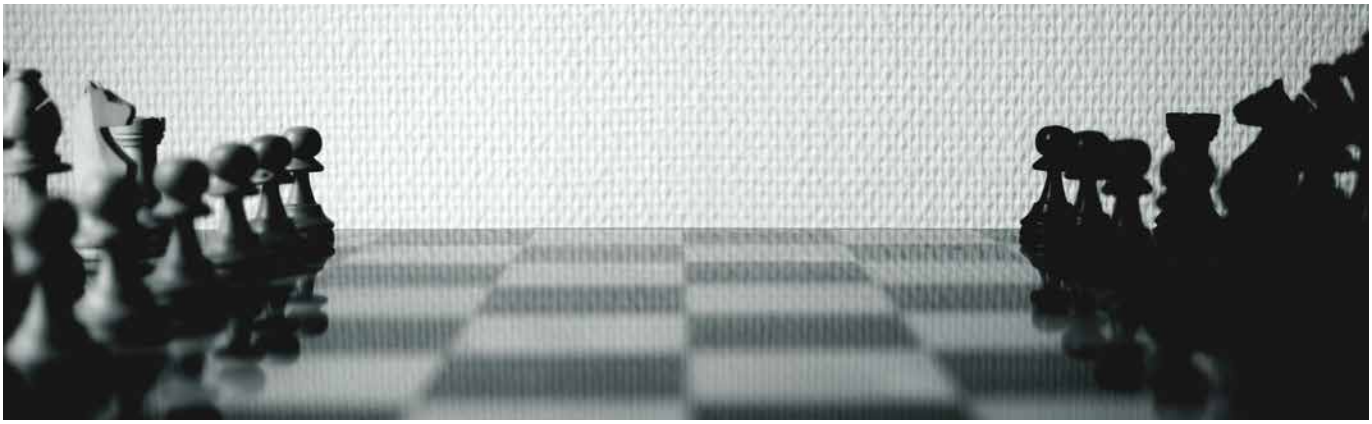
LOGIC BOMBS

Once installed by any of the previously discussed methods, Logic Bombs sit dormant and virtually undetectable until a particular condition is satisfied. For example, a certain date is reached, or a certain user logs in. Once the condition is satisfied, it will carry out further instructions.

RANSOMWARE

After being installed, ransomware encrypts a portion of a computer system, the entire computer system or even an entire network. The user then is presented with a ransom note that provides instructions on how to pay and receive a decryption tool, typically payments are made with cryptocurrencies such as Bitcoin. Once files are encrypted, there is no way to decrypt them without the decryption tool. Some ransomware also will present a deadline and begin deleting files if payment is not received.

Phone: 866-793-8232
Email: solutions@advantage.tech



Botnet

A network of hijacked computers a hacker uses for attacking other networks, spending spam or performing calculations such as cryptocurrency mining or cracking stolen passwords.

Man In The Middle

A technique where an attacker intercepts a network connection then relays it to the destination. This enables the attacker to see everything sent over the network without being detected by the user.

Pharming

A bad actor sets up fraudulent websites to trick unsuspecting users into installing software or entering credentials or financial information. For example, the site could claim the user has a virus and offer a free virus removal which actually is malware. Or the fake site could look identical to PayPal to trick a user into entering their PayPal credentials, which is then harvested by the bad actor to access the user's PayPal account.

Phishing

The attacker sends out emails that appear to be legitimate but have links to pharming sites or attachments that contain malware.

Social Engineering

Conducted both online and offline, social engineering encompasses techniques used by bad actors to trick a person into providing key information needed for a scheme. This could be a phone call from someone claiming to be with the Social Security Administration requesting you verify your Social Security number or pretending to be an old friend on social media to trick a person into telling them security information such as the street they grew up on or their mother's maiden name. It also can include eavesdropping on a local coffee shop to get key information on the business, such as when an executive is out of town or an administrative assistant's name.

Spear Phishing

A highly targeted phishing attack with information typically acquired through social engineering. Due to the specific information presented in the email, spear phishing attacks can be incredibly effective.

Phone: 866-793-8232
Email: solutions@advantage.tech

THE RESULTS

Depending on the actors and their tactics, the impact of cybercrime can be **personally and financially devastating.** It can range from public humiliation to bankruptcy. It could be that the desired result is to embarrass you by releasing private emails or to wipe out your data because they think it's funny. **But many times, a cybercriminal just wants cash and will go to almost any length to get it.**

First, it's important to understand these actors and their tactics. Then, we can look into tried and true cybersecurity practices that will help you protect yourself and your organization.

Identity Theft

Financial Theft

Blackmail

Public Humiliation

Corporate Espionage

Legal Costs

Phone: 866-793-8232
Email: solutions@advantage.tech

4

HOW TO PROTECT YOURSELF

Seven Cybersecurity Fundamentals

1. Mindset

The single most important protection from cybercrime is the right **mindset.**

You always should view yourself as a target and be suspicious of every interaction you have on the internet. Every email, every website that asks for personal information and every free app should get a second look. Just because you're paranoid doesn't mean they're not out to get you.

Extend your suspicion into the real world as well. Shred financial documents as well as any other documents with personal information. Don't leave passwords on sticky notes. Don't discuss sensitive information in public.

2. Policies and Procedures

Once you get your mindset right, the base level of cybersecurity comes down to your **Policies and Procedures.** Policies are the way things are supposed to work, while Procedures are the enforcement mechanism for your Policies.

An example of a Policy would be Password Construction Policy, where passwords are required to be at least 10 characters with one number and one special character. A Procedure would be a setup on your server that requires the user to enter a password with those conditions and reject anything doesn't meet the minimal standards.

Policies and Procedures can be complex and industry specific. You should always have a qualified compliance and cybersecurity firm assist in the development of your Policies and Procedures to ensure compliance and effectiveness.

Your Policies and Procedures will govern every other part of your cybersecurity plan.

Phone: 866-793-8232
Email: solutions@advantage.tech

3. Threat Management

All information systems are vulnerable to attack. Hackers constantly are discovering new exploits and cybercriminals are developing these exploits into threats. There never will be a way to eliminate these threats entirely, but there are several must-have technologies that can minimize your risk and exposure.

A FIREWALL

An appliance that sits between your network and the Internet and scans all data that passes through. The firewall is able to stop a variety of threats and prevent certain types of network traffic that is susceptible to attacks.

GATEWAY ANTIVIRUS

Monitors network traffic and can prevent malware from entering your network.

GATEWAY ANTISPAM

Scans emails to intercept spam and phishing emails.

CONTENT FILTERING

Prevents users from accessing certain content, such as websites that are known to harbor malware.

DATA LOSS/LEAK PREVENTION

Prevents certain types of data from being transferred outside of the network, stopping it from reaching the Internet.

Many of these tools can be deployed from a single appliance. A qualified cybersecurity firm will be able to provide you with recommendations for the type of appliance that would be appropriate for your network.

LOGGING

All threat management systems should log events. These logs are important to identify new types of threats and reconstruct events should a breach occur.

SECURITY PATCHES

Hackers constantly are discovering exploits in threat management systems, and vendors are constantly working on new patches to eliminate those exploits. These security patches are absolutely critical and should be installed regularly and coordinated with best-of breed patch management solutions.

Phone: 866-793-8232
Email: solutions@advantage.tech

4. Endpoint Protection

Devices on your network are known as endpoints. These endpoints include workstations, laptops, mobile devices and tablets, including devices that are only connected wirelessly. Other devices that aren't thought of as computers are also endpoints, such as printers, security cameras, smart meters and even smart lightbulbs. Any device on your networking is an endpoint and potential route for a cybercriminal to gain access to your network.

STRONG PASSWORDS

The most important piece of endpoint protection is the use of strong passwords, any device on a network should require a password to gain access. The password can be a PIN number or biometrics scan, such as a fingerprint or facial recognition scan.

A strong password is not a literal word, it's a series of characters that should be easy to remember but hard to guess. A great method for developing a strong password is to start with a phrase such as, "Four score and seven years ago," replace some parts with numbers; "4ScoreAnd7YearsAgo." Then add characters to satisfy your company's password policy. "!4Score&7YearsAgo!" is a complex, hard to guess but memorable password.

TWO-FACTOR AUTHENTICATION

Is a step beyond passwords in which gaining access to a system requires two separate things. Typically, the two factors are ***something you have and something you know.*** *So, accessing an account would require a fingerprint scan (something you have) and a password (something you know). Or a PIN sent to your phone (something you have) and a password (something you know).*

You should enable two-factor authentication for any service that offers it.

HOST-BASED FIREWALL

A software firewall that runs on the endpoint device and prevents anything malicious from access the system.

ANTIVIRUS

Software that runs on the on the endpoint and prevents malware from accessing the system.

Phone: 866-793-8232
Email: solutions@advantage.tech

4. Endpoint Protection (continued)

ENCRYPTION

The process of encoding information so that only authorized individuals can access it. Encryption should be used at all levels on endpoints, including encrypting hard drives, removable storage, and all network traffic. Even if a device is stolen, if all the data is encrypted, it will be worthless to a cybercriminal.

Websites that are accessed with HTTPS rather than HTTP are encrypted. You should always opt to use the HTTPS version of a website if available. Always use HTTPS if you are submitting sensitive information such as credit card numbers, if the site does not have an HTTPS option do not submit any sensitive information to it.

SECURITY PATCHES

All endpoint devices are potential targets for cybercriminals, including smart-home devices such as cameras, thermostats, even light bulbs. If it is on a network or is capable of accessing a network, it is at risk. Even specific software can be targeted. This is why consistent security patching on all endpoint devices and software is paramount. Check for security updates and install them regularly.

GROUP POLICY

Devices and software that are on a network can have their activity governed by a centralized controller. This controller defines the Group Policy and prevents any unauthorized activity on the network based on the role of the employee.

For many of the tools and software required for endpoint protection, such as antivirus and encryption, there are lots of options on the market. A qualified cybersecurity firm will be able to provide you with recommendations. Developing Group Policies that align with your industry's Policies and Procedures will also require a level of expertise.

Phone: 866-793-8232
Email: solutions@advantage.tech

5. Event Monitoring

Even the most sophisticated and thorough threat management and endpoint protection programs can be useless if their network activity goes unmonitored. **Trained experts need to monitor logs and reports from hardware and software to identify potential attackers before they penetrate the network.**

A consistent and rigorous event monitoring program must be maintained to rapidly detect, contain and hunt down advanced threats before they gain a foothold in your network and cause serious damage or a breach.

6. Training and Education

Thankfully, you already have a great start on your education by reading this manual! You also can share it with colleagues and continue to stay up to date by visiting www.advantage.tech/cybersecurity for all of the latest, relevant cybersecurity news and tips.

As threats continue to evolve, we have to continue our education and apply new techniques that are discovered daily to become aware of new vulnerabilities and prevention methods.

Everyone in your organization should read and understand the Policies and Procedures and have a base understanding of cybersecurity.

A qualified cybersecurity firm also can assist in development of testing methods where faux malware, pharming, and phishing can be deployed on your network. Discover who is most likely to become a victim and help them with additional training and tools. Annual testing should be a regular event in your organization.

Phone: 866-793-8232
Email: solutions@advantage.tech

7. Business Continuity

Even with the most sophisticated cybersecurity plan in place, there's no way to completely eliminate the threat of cybercrime. Hackers and criminals are constantly looking for new ways to penetrate networks, steal data and generally wreak havoc. So contingency plans should be developed to mitigate damage and ensure business continuity.

First and foremost, **the best contingency plan is the one you'll never have to use.** To reduce the chances of falling victim to cybercrime, an annual cybersecurity plan assessment should be conducted by a qualified compliance and cybersecurity firm. The assessment will review all your policies and procedures, ensure your threat management and endpoint protection systems are adequate and up-to-date and find any gaps that need to be address.

Along those same lines, it's important to **stress test** the people of your organization and the technology.

A **penetration test** is an attempt by a cybersecurity expert to hack into your network, and thus identify any holes in your cybersecurity. By identifying the holes before a cybercriminal does, you can take steps to patch them before you are breached.

Pharming and phishing tests should be done routinely as well. These tests will identify individuals with gaps in their knowledge and awareness. Further training and education can then be employed to bring them up to speed.

Still, the worst always is possible. And the best defense against the worst-case-scenario of total data loss is **a robust backup and recovery solution.** Basic backups store your data to ensure you don't lose it, but the most important part for business continuity is recovery. If you have a backup but it takes a week to restore your data, that means you're out of business for a week. A robust backup and recovery should restore quickly, efficiently and provide access to the data even before the restoration is complete.

To accomplish this, **the backup needs to be onsite and offsite.** Onsite backups provide rapid recovery and access to the data. Offsite backups provides protection against catastrophic events such as theft, vandalism, fire or flood. A robust offsite backup will also provide access to the data via the cloud.

If there is a data breach, it's means you already have been caught off guard. The last thing you need to deal with is the chaos that follows when no one knows what to do next. Instead, **plan ahead** and create an Incident Response Plan. By coordinating all of your departments and having them primed and ready, you greatly can reduce the impact of a breach. It's even possible you could stop the attackers in their tracks before too much damage is done.

Part of your Incident Response Plan should include crisis communication, to ensure you are able to get out in front of any negative media coverage. Show your customers that you are proactive, and they will be quicker to forgive.

A qualified compliance and cybersecurity firm can help you develop your business continuity plan. It can help you coordinate your teams and provide you with recommendations on testing, training and backup solutions.

Phone: 866-793-8232
Email: solutions@advantage.tech

5

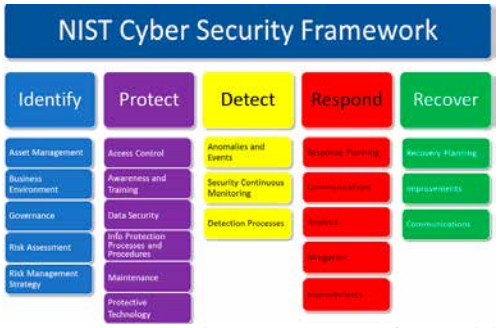
WHERE TO START

Putting it all together

THE UNFORTUNATE REALITY TODAY IS THAT THERE ARE ONLY TWO TYPES OF COMPANIES WHEN IT COMES TO CYBERATTACKS: THOSE THAT HAVE BEEN VICTIMS, AND THOSE THAT WILL BE. SO, WHAT CAN YOU DO TO PROTECT YOURSELF, AND YOUR CLIENT'S DATA?

The best recommendation is to rely on a trusted technology adviser with cybersecurity experts to help you establish proper safeguards against a cyberattack, and help you prepare an adequate response and recovery plan, should an attack occur. **You didn't go into business to take care of computers, and cybersecurity is definitely not a job for the do-it-yourselfer.** However, if you are the DIY type, there are some things that you can do to strengthen your overall cybersecurity posture and help you prevent and recover from an attack.

From an overall strategy perspective, you should look at cybersecurity as a process with many facets and components. **Cybersecurity is not a "one and done" type of project,** but is instead and ongoing effort. To assist in this sometimes large and daunting process, the **National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF)** was published in response to Presidential Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," which called for a standardized security framework for critical infrastructure in the United States.



The NIST CSF is recognized by many as an excellent resource to help improve the security operations and governance for public and private organizations. **The NIST CSF is organized into five core functions also known as the Framework Core.** The functions are organized concurrently with one another to represent a security lifecycle.

Each function is essential to a well-operating security posture and successful management of cybersecurity risk. Definitions for each function are as follows.

Identify

Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

Protect

Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

Detect

Develop and implement the appropriate activities to identify the occurrence of a security event.

Respond

Develop and implement the appropriate activities when facing a detected security events.

Recover

Develop and implement the appropriate activities for resilience and to restore any capabilities or services that were impaired due to a security event.

If you want to increase their overall cybersecurity posture, investigate and implement the NIST CSF and its appropriate security controls. Find out more at https://www.nist.gov/cyberframework

Advantage Technology has cybersecurity and compliance experts who can help guide you through the NIST CSF analysis and implementation.

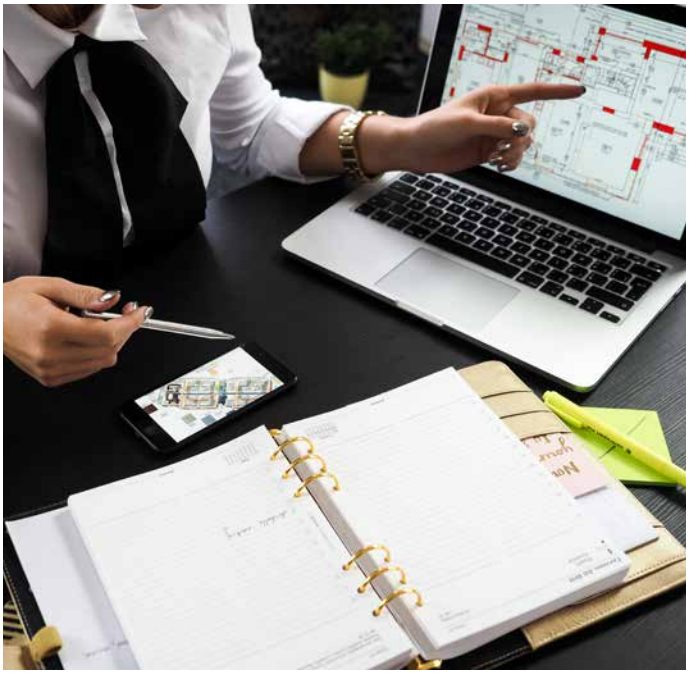
Phone: 866-793-8232
Email: solutions@advantage.tech

ADVANTAGE IT DISCOVERY

IF YOU'RE NOT QUITE READY FOR A DEEP DIVE INTO THE NIST CSF, AND YOU JUST NEED A BASIC UNDERSTANDING OF YOUR CURRENT NETWORK STATE, ADVANTAGE TECHNOLOGY OFFERS OUR ADVANTAGE IT DISCOVERY FOR LESS THAN $100.

The **Advantage IT Discovery** consists of a high-level view of your network with a network assessment **Risk Report** and site survey. Then we follow that up with a fully customized, comprehensive list of **Advantage Managed Services.**

Advantage Managed Services are proactive IT services curated by our experts to keep your networking running at peak performance and protect your data from disaster. There's no obligation to subscribe to any of these managed services, but once you see how they can benefit your business, you'll want every single one.



The Risk Report scans your entire network and identifies things such as inactive computers, lack of anti-virus, poor password protocols, insecure listening ports, unsupported operating systems, low disk space, Internet speed and many other key network management factors. This information is incredibly valuable for both identifying immediate needs and planning future changes, such as hardware replacement, cloud transitions, and software upgrades.*

Your technology should **add value to your business, not devour precious resources** like your time, money and sanity. The Advantage IT Discovery is an excellent first step in properly understanding and managing your network.

*The Risk Report is for informational purposes only. While the data gathered is valuable for maintenance and planning, it should not be considered a comprehensive network evaluation or security assessment

Phone: 866-793-8232
Email: solutions@advantage.tech

FINAL WORDS

Contact Us Now

950 Kanawha Blvd E. #100
Charleston, WV 25301

416 S. Conococheague St. #3
Williamsport, MD 21795

600 Marketplace Ave, #102
Bridgeport, WV 26330

2333 Alexandria Dr. #211
Lexington, KY 40504

866-793-8232

solutions@advantage.tech

www.advantage.tech

Connect With Us

AdvantageTechnologyWV

company/advantage-technology

advantagetechwv

CONTACT ADVANTAGE TECHNOLOGY FOR ALL YOUR CYBERSECURITY AND TECHNOLOGY NEEDS

Advantage Technology is the largest full-service Information Technology consulting company headquartered in West Virginia, with offices in Charleston and Bridgeport, Williamsport, MD and Lexington, KY. We provide IT services for over 850 professional companies and organizations across the United States and Canada.

Everyone here at Advantage Technology would like to thank you for reading this manual and taking the first steps toward taking cybersecurity seriously. We hope you take this knowledge to the next level and contact us for your cybersecurity needs. You can call us at **866-793-8232,** email us at **solutions@advantage.tech** or visit **www.advantage.tech** for all the latest news and information.

We're looking forward to hearing from you. Stay safe out there.

Professional Services

At its core, Advantage Technology is a company that specializes in technological solutions. From datacenter installs to server consolidations and from help desk support to custom software development, we can achieve any goal. Our technicians hold various degrees and industry-recognized certifications from VMware, Microsoft, Dell EMC, SonicWALL, Aruba Networks, Extreme Networks and others.

Cybersecurity

In recent years, massive data breaches have been making headlines all over the world. From these headlines, one thing is clear; many organizations do not give enough attention to cybersecurity. At Advantage Technology, we're dedicated to addressing this problem and consulting with both large and small businesses and organizations to keep their data and their client's data, safe and secure.

Cloud Computing

The fastest growing sector of IT, Cloud Computing utilizes 3rd party, internet connected data centers as a platform for your computational needs rather than managing physical resources. Having your computational needs handled in the Cloud provides an incredible amount of flexibility, scalability, and access.

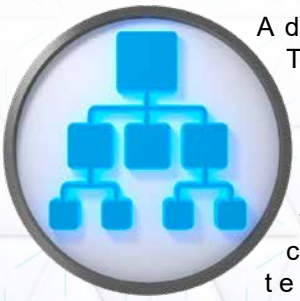
Managed Services

Technology should add **VALUE** to your business, not devour precious resources like time, money and sanity. Advantage Managed Services are proactive IT services curated by our experts to keep your network running at peak performance, maintain critical services and protect your data from disaster.

Telecommunications

Communication is the lifeblood of all business and getting the right phone system is a critical component of any communication strategy. From installing cable to choosing the right handset, Advantage Technology handles all the stages of installation and support.

Structured Cabling



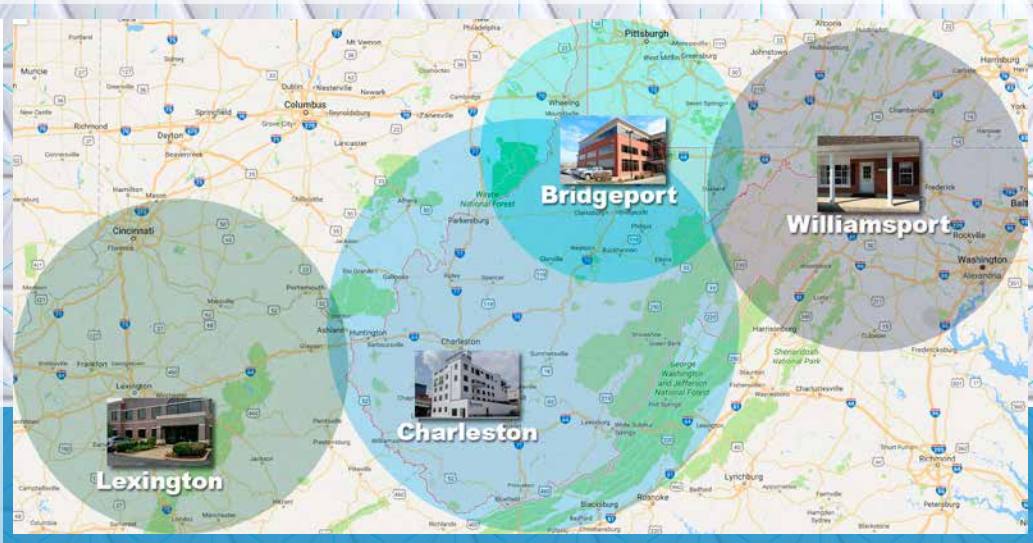
Advantage Technology is a licensed and insured contractor with highly trained cabling technicians and engineers. Our staff has decades of experience working in construction cabling and includes BICSI certified technicians, including a Registered Communications Distribution Designer (RCDD).

Charleston Headquarters
950 Kanawha Blvd E, #100
Charleston, WV 25301

Williamsport Office
416 South Conococheague #3
Williamsport, MD 21795

Bridgeport Office
600 Marketplace Ave #102
Bridgeport, WV 26330

Lexington Office
2333 Alexandria Dr. #211
Lexington, KY 40504



www.advantage.tech

866-793-8232 • 950 Kanawha Blvd E #100 • Charleston, WV 25301 • www.advantage.tech