COMPUTER SERVICES

Cyber Security

Presented by: Rick & Ben Raesz with RCOM Computer Services

A little about RCOM Computer Services

We are a 41-year-old IT Computer Services Company with offices in Texas and Colorado. We provide a host of managed computer services for companies like yours and we are your Cyber Security Authority.

Oh and IECRM has been one of our clients and best friends for years. RCOM has provided Managed IT Services for the IEC organization for over 30 years.

Times have changed

A new year is a great time for new beginnings, and there's no better time to take a hard look at upping your security game. If your organization has been relying on security through obscurity ("we're too small or too unimportant for attackers to bother"), you're living on borrowed time. Industry experts are predicting that 2023 will bring new and more sophisticated hacks and attacks, more dangerous forms of malware, the growth of hacktivism, and a surge in cyberthreats. You are not too small to be compromised, your just too small to make the news when it happens to companies like yours.

That's the bad news. The good news is that your security strategy (or lack thereof) doesn't have to stay where it is. You can take that first step, right now, toward getting it to where it needs to be.

Both individuals and entities tend to be resistant to change, even when it's sorely needed – maybe especially when it's sorely needed. Companies tend to focus on the data and the numbers and take for granted their network is safe because nothing has happened to it yet. If you own a small to mid-sized organization that has been around for a few decades, it's likely that security wasn't baked in from the beginning but was tacked on later almost as an afterthought. There's a problem with that.

If you have firewalls and a good antivirus/antimalware solution, that's a good beginning, but it's only the first step toward protecting your network and systems – and thus your real assets: your intellectual property, company financial data, employee and customer personal data, etc. – from the bad guys.

How many of you use cell phones or mobile devices laptops, tablets and so forth outside of your business office? Your cell phone, laptop or any mobile device with internet connectivity is an open door to your personal and customer data, intellectual property, and trade secrets that make up your unique services to your customers that you can't afford to lose. How many would agree that keeping your car in your garage is more secure? We probably all would, but ANY device outside the walls of your organization or house, if you will, is exponentially more susceptible to being compromised because they are not protected like your internal company network.

You're probably aware that there are weaknesses in your security implementation that are ripe for exploitation, but if "it just grew that way," rebuilding a security program means upsetting some apple carts. It's a daunting task in more ways than one. It involves getting executive buy-in, finding the funding (not easy in an inflationary environment), assessment, planning, testing, implementation, reassessment and fine-tuning, and ongoing improvement. Just thinking about all that is enough to make you want to just keep crossing your fingers and hoping your luck holds out. **It won't!!!**

Don't let tragedy define purpose! When tragedy shows up, I can promise you this, you will realize the things you didn't realize when you had the opportunity. Like "I should have addressed this before it became a life-threatening problem for my business. I just never thought it would happen to us."

There are those that have been hacked or compromised and those that will be. It is no longer those that won't!

Cyber attackers are increasingly targeting small and mid-size businesses . Because you can't afford to pour as much money into security as large enterprises do, criminals see your company as low-hanging fruit. According to some statistics, almost half (46%) of breaches impacted small businesses in 2021/2022, and over 60% of SMBs experienced attacks.

Do you think your company doesn't have the money to upgrade your security? An attack will likely cost much more. According to the National Cybersecurity Alliance, as many as 60% of small businesses go out of business following a cyberattack. The average cybersecurity insurance claim cost for a ***small to medium enterprise is $345,000***

Don't let Cyber Insurance give you a false sense of security. The average total claim payout for a cyber security claim is 28 to 40%. We know how insurance companies will do whatever they can to find someone else responsible and now that includes the MSP (Managed Service Provider) that is contracted to help protect you.

What is Cybersecurity?

Cyber security is the application of technologies, processes, and controls to protect electronic systems, networks, programs, devices, and data from malicious cyber-attacks. It's also known as information technology security or electronic information security.

It aims to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems, networks, and technologies.

The term “cybersecurity” applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.

Why is Cybersecurity Important?

The importance of cybersecurity is primarily driven by the following factors.

Cyber Attacks Are Increasingly Sophisticated

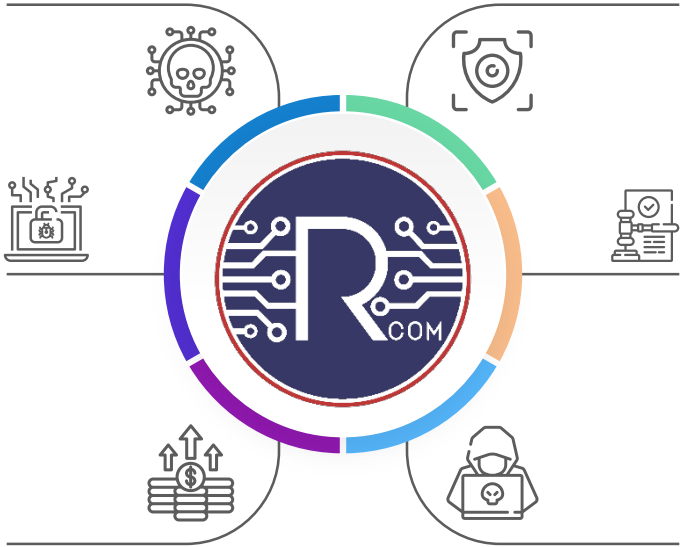
Cyber-attacks are evolving daily, and attackers use an ever-expanding variety of tactics and advanced tools. These include social engineering, malware, DDoS, and ransomware.

Widely Available Hacking Tools

A wide range of hacking tools and tactics are available online for free. Your cyber attacker today could very well be someone with limited digital skills.

Rising Cost Of Cyber Security Breaches

Fines and lost business are just one aspect of the rising financial cost of security breaches. There are also expenses associated with containing the impact, disaster recovery, closing loopholes, acquiring new security systems, and repairing the organization's reputation.



Cyber Security Is A Critical, Board-level Concern

New regulations and reporting requirements make cyber security risk oversight a challenge. The board needs assurance from management that its cyber risk strategies will reduce the risk of attacks and limit financial and operational impacts.

Compliance Issues

Regulations such as the General Data Protection Regulation (GDPR) require organizations to deploy security measures to protect sensitive information. Failure to comply would lead to substantial fines and legal action.

Cyber Crime Is A Big Business

Cyberattacks can have social, ethical, or political motives. Nevertheless, the vast majority are driven by financial intentions. Cybercrime is a multibillion-dollar industry.

The Importance of Cybersecurity

1. Eliminating Threats

Cyber security provides comprehensive digital protection to your business. This allows your employees to safely surf the internet when they need it and ensure that they aren't at risk from threats.

2. Cyber Attacks

A Cyber Security Risk Assessment (CSRA) would assess your existing security infrastructure and then suggest powerful solutions to ensure your network is secure from all kinds of cyber attacks.

4. Safe Work Environment

With good security solutions in place, your employees can have a safe working environment with little downtime due to a cyber-attack.

3. Data Protection

Robust firewalls, anti-malware solutions, and customized filters ensure that your data is always safeguarded.

Types of Cybersecurity Threats

Malware

Phishing

Spear Phishing

Man in the Middle Attack

Denial of Service Attack

SQL Injection

Zero-Day Exploit

Advanced Persistent Threats

Ransomware

DNS Attack

Types of Cybersecurity Threats

Malware

Malware attacks are the most common cyber security threats. Malware is defined as malicious software, including spyware, ransomware, viruses, and worms, which gets installed into the system when the user clicks a dangerous link or email. Once inside the system, malware can block access to critical components of the network, damage the system, and gather confidential information, among others.

Spear Phishing

Spear phishing is a more sophisticated form of a phishing attack in which cybercriminals target only privileged users such as system administrators and C-suite executives.

Phishing

Cybercriminals send malicious emails that seem to come from legitimate resources. The user is then tricked into clicking the malicious link in the email, leading to malware installation or disclosure of sensitive information like credit card details and login credentials.

Types of Cybersecurity Threats

Denial of Service Attack

Denial of Service attacks aims at flooding systems, networks, or servers with massive traffic, thereby making the system unable to fulfill legitimate requests. Attacks can also use several infected devices to launch an attack on the target system. This is known as a Distributed Denial of Service (DDoS) attack.

Man in the Middle Attack

Man in the Middle (MitM) attack occurs when cyber criminals place themselves between a two-party communication. Once the attacker interprets the communication, they may filter and steal sensitive data and return different responses to the user.

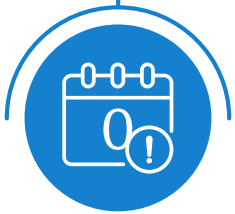
SQL Injection

A Structured Query Language (SQL) injection attack occurs when cybercriminals attempt to access the database by uploading malicious SQL scripts. Once successful, the malicious actor can view, change, or delete data stored in the SQL database.

Types of Cybersecurity Threats

Zero-day Exploit

A zero-day attack occurs when software or hardware vulnerability is announced, and the cybercriminals exploit the vulnerability before a patch or solution is implemented.



Advanced Persistent Threats (APT)

An advanced persistent threat occurs when a malicious actor gains unauthorized access to a system or network and remains undetected for an extended time.

Ransomware

Ransomware is a type of malware attack in which the attacker locks or encrypts the victim's data and threatens to publish or block access to data unless a ransom is paid. Learning more about ransomware threats can help companies prevent and cope with them better.

DNS Attack

A DNS attack is a cyberattack in which cybercriminals exploit vulnerabilities in the Domain Name System (DNS). The attackers leverage the DNS vulnerabilities to divert site visitors to malicious pages (DNS Hijacking) and remove data from compromised systems (DNS Tunneling).

What is the difference between a Breach and Compromise?

Breach:

In the IT world, the Breach occurs when someone gains access to your network, local computer or mobile device.

Compromise:

The Compromise is when the bad guys steal your data and sell it on the black market, encrypt your data with Ransomware and hold you hostage, or utilize it for their own financial gain.

What is the difference between a Breach and Compromise?

In the military they teach special forces “The bottom of your foot or an explosive device causes the breach and the WEAPON that you chose determines the outcome of the compromise.”

This is the approach RCOM takes by providing you the managed IT services and weapon(s) you need to protect your network, customer and personal data, and intellectual property.

Cyber Threat Actors

Here are some of the common sources of cyber threats:

1) Nation States

Cyber attacks by a nation can inflict detrimental impact by disrupting communications, military activities, and everyday life.

2) Criminal Groups

Criminal groups aim to infiltrate systems or networks for financial gain. These groups use phishing, spam, spyware, and malware to conduct identity theft, online fraud, and system extortion.

3) Hackers

Hackers explore various cyber techniques to breach defenses and exploit vulnerabilities in a computer system or network. They are motivated by personal gain, revenge, stalking, financial gain, and political activism. Hackers develop new types of threats for the thrill of challenge or bragging rights in the hacker community.

4) Terrorist Groups

Terrorists conduct cyber attacks to destroy, infiltrate, or exploit critical infrastructure to threaten national security, compromise military equipment, disrupt the economy, and cause mass casualties.

5) Hacktivists

Hacktivists carry out cyberattacks in support of political causes rather than for financial gain. They target industries, organizations, or individuals who don't align with their political ideas and agenda.

6) Malicious Insiders

Insiders can include employees, third-party vendors, contractors, or other business associates who have legitimate access to enterprise assets but misuse their access to steal or destroy intellectual property for financial or personal gain.

7) Corporate Spies

Corporate spies conduct industrial or business espionage to either make a profit or disrupt a competitor's business by attacking critical infrastructure, stealing trade secrets, and gaining access.

Interesting Fact

The majority of “Black Hat” hackers are part of terrorist groups to fund their dastardly deeds.

The rest are comprised mostly of people that have been playing with computers in their parents’ basements since they were 5 years old.

Types of Cyber Security

Network Security: It involves implementing the hardware and software to secure a computer network from unauthorized access, intruders, attacks, disruption, and misuse.

Application Security: It involves protecting the software and devices from unwanted threats.

Cloud Security: It involves protecting the information stored in the digital environment or cloud architectures for the organization.

Data Security: It involves implementing a strong data storage mechanism to maintain the integrity and privacy of data, both in storage and in transit.

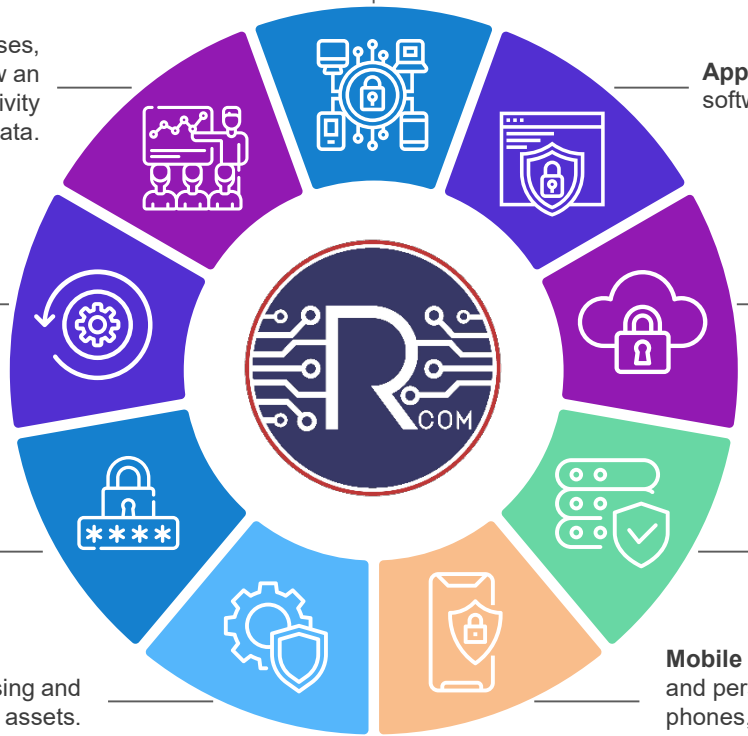
Mobile Security: It involves securing the organizational and personal data stored on mobile devices such as cell phones, computers, tablets, and other similar devices against various malicious threats.

Operational Security: It involves processing and making decisions in handling and securing data assets.

Identity management: It deals with the procedure for determining the level of access that each individual has within an organization.

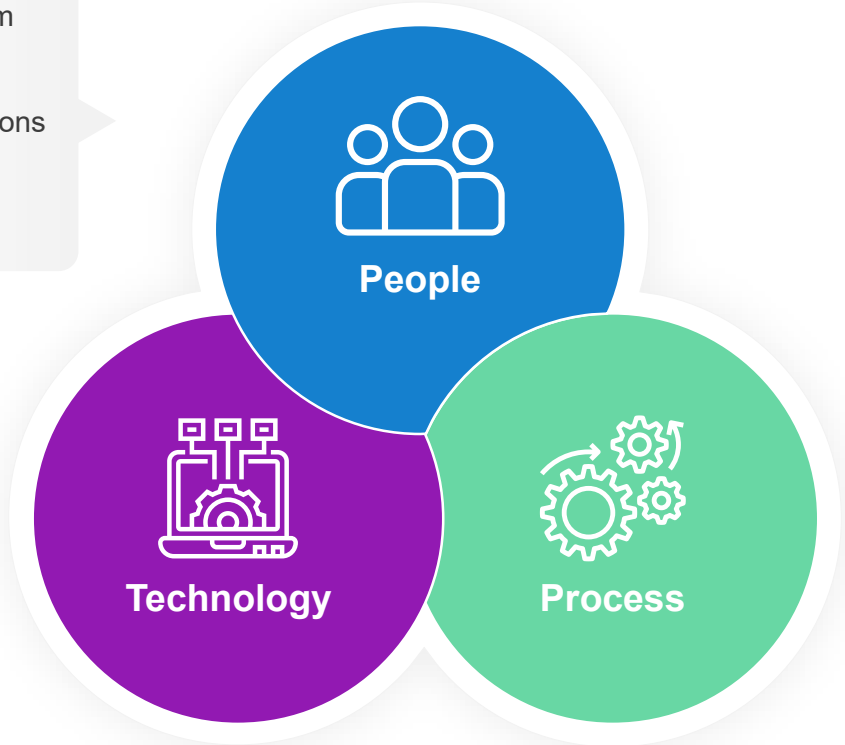
Disaster Recovery and Business Continuity Planning: It deals with the processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data.

User Education: It deals with the processes, monitoring, alerts, and plans to how an organization responds when any malicious activity is causing the loss of operations or data.



The Three Pillars of Cyber Security

- Your weakest link is your Team
- Cyber hygiene
- Training & awareness
- Professional skills & qualifications
- Written procedures
- Authorization control
- Physical security



- Antivirus
- Firewalls
- Intrusion detection systems
- SW updates, patches
- Testing
  - Cyber Security Risk Assessment
  - Functional testing
  - Vulnerability scanning
  - Penetration test

- Management systems
- Policies, procedures
- Handling of vendor/third parties
- Drills & audit regimes
- State and Federal governance and compliance regulations

Cyber Security vs. Information Security

Cybersecurity

It is the practice of shielding the data on the internet from outside of the resource.

It is about the capacity to protect the use of cyberspace against cyber attacks.

Cybersecurity is combating cyber crime, cyber fraud, and law enforcement.

Cybersecurity identifies cyberspace threats.

Cybersecurity to secure everything in the cyber domain.

VS

Information Security

It is all about securing data, access and data alteration from unauthorized users.

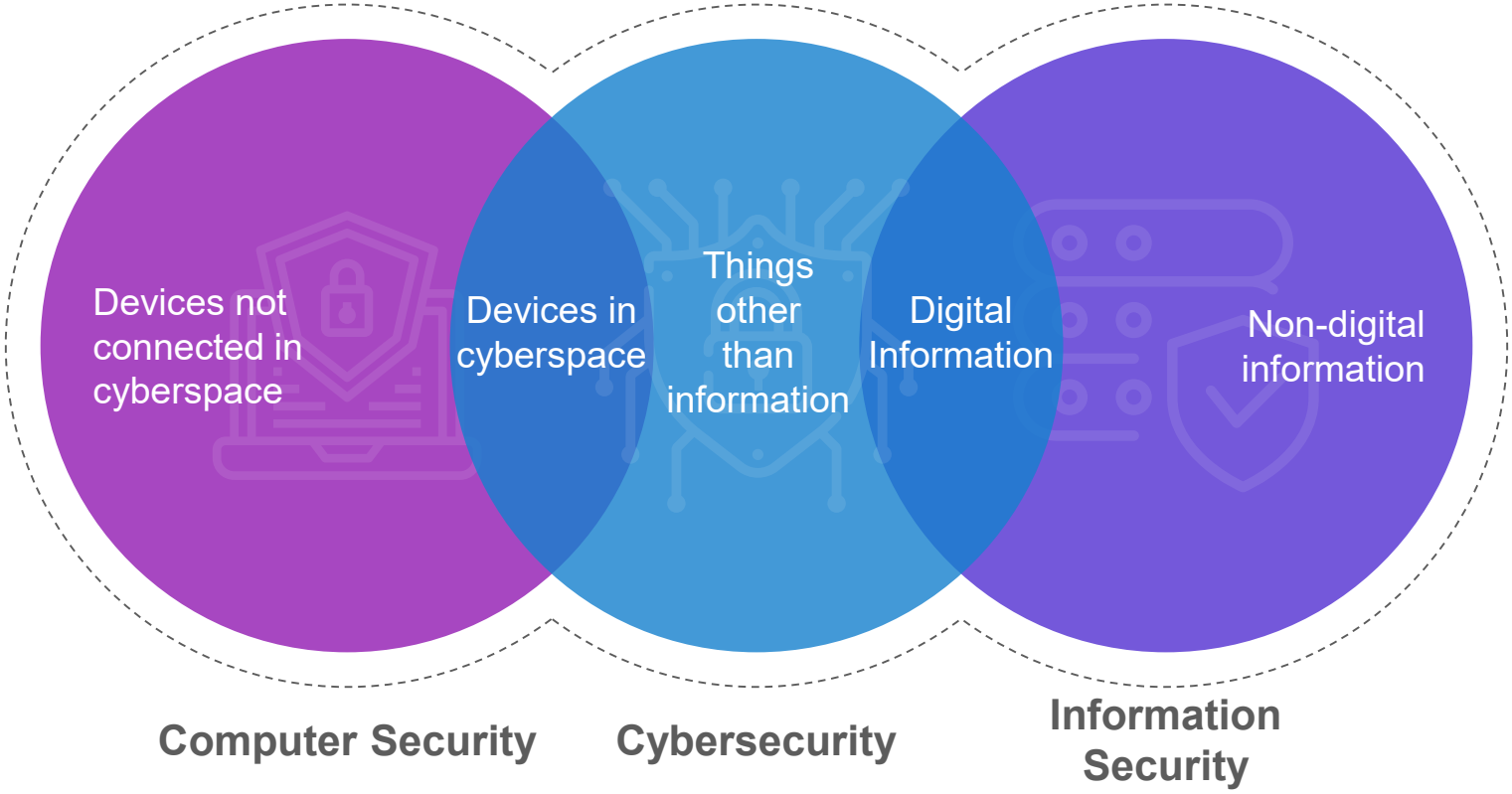
It deals with data security from some type of threat.

Information security strives against unauthorized entry, altering and undermining access.

The security of information deals with data protection from some sort of attack.

Information security is for records, regardless of the domain.

Cyber Security vs. Information Security vs. Computer Security



Cyber Security vs. Network Security

Cybersecurity

Cyber security is a subset of information security.

It is the practice of protecting internet-connected systems and networks from digital attacks.

It protects the organization from all kind of digital attacks from the cyber realm.

Network protection, applications, up-to-date information, comes under cyber security.

A cyber security professional serves as an expert on cyber security protections, detection, and recovery.

VS

Network Security

Network security is a subset of cyber security.

It is the act of protecting files and directories in a network of computers against misuse, hacking, and unauthorized access.

It is all about protecting the organization's IT infrastructure from all kinds of online threats.

ID and passwords, internet access, firewalls, backup, encryption, comes under network security.

The job of a network security professional revolves around protecting IT infrastructure of the organization.

Cybersecurity Compliance

Types of Cybersecurity Compliance

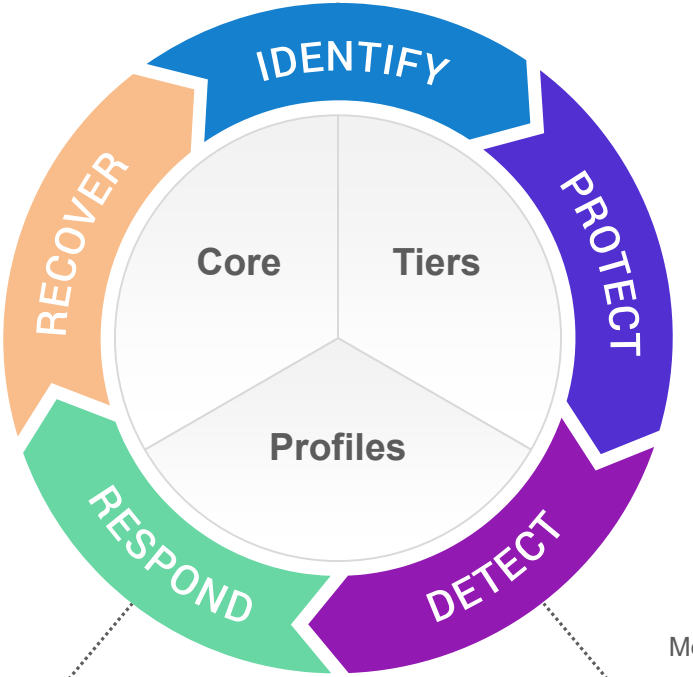
Cybersecurity Compliance

PCI DSS	PCI DSS (Payment Card Industry Data Security Standard). It is a set of security controls required to implement to protect payment account security. It is designed to protect credit card, debit card, and cash card transactions
ISO 27001/27002	ISO 27001/27002 (International Organization for Standardization). Best practice recommendations for information security management and information security program elements.
CIS (Critical Security Controls)	They are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks.
NIST Framework	NIST is the National Institute of Standards and Technology at the U.S. Department of Commerce. A Framework for improving critical infrastructure Cybersecurity with a goal to improve organization’s readiness for managing cybersecurity risk by leveraging standard methodologies and processes.
HIPAA	Is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.
FTC	The FTC Safeguards Rule requires covered companies to develop, implement, and maintain an information security program with administrative, technical, and physical safeguards designed to protect customer information.

NIST Cyber Security Framework

Cybersecurity Framework's Five Functions

1. Identify Function:
Start by listing all equipment, software, vendors, and data you use. Create a district cybersecurity handbook and update school board policies concerning employee and student records.



2. Protect Function:
Take steps to track traffic, encrypt sensitive data, update software regularly, change passwords periodically, and train employees and students about cybersecurity.

3. Detect Function:
Monitor computers and web use for authorized access and identify any unusual activities.

4. Respond Function:
Establish a business continuity plan, notify anyone whose data may be compromised, report attacks to authorities, contact your cyber insurance carrier, and update the cybersecurity handbook based on experience.

5. Recover Function:
After an incident, repair any equipment that was affected, and keep everyone involved up to date with your response and recovery actions.

The Top Cyber Security Challenges

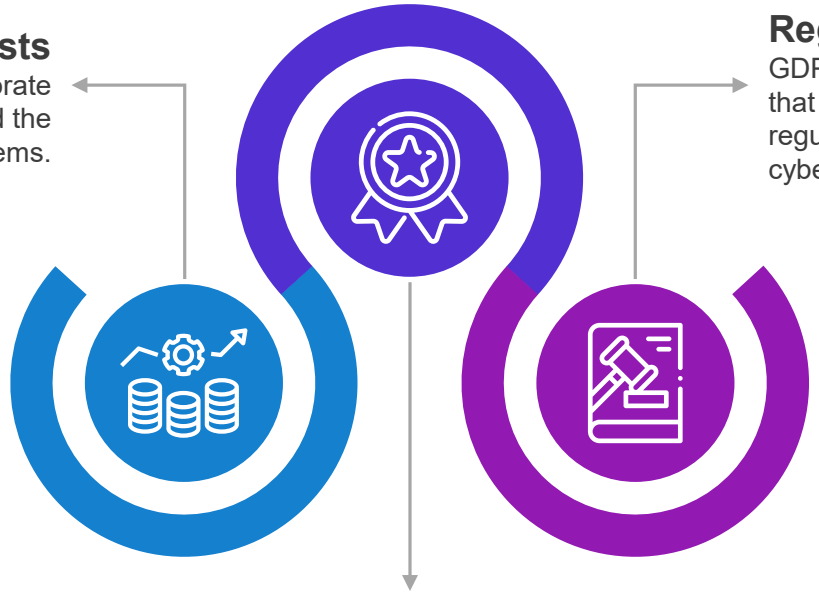
- Ransomware Attacks
- Cloud Services Attacks
- Blockchain and Cryptocurrency Attacks
- Supply Chain Attacks
- Smartphones Malware Attacks
- IoT (Internet of Things) Attacks
- Machine learning and AI Attacks
- Attacks on Remote Work Environments
- Phishing and Insider Attacks
- Software Vulnerabilities
- Bring Your Own Device (BYOD) Threats
- Outdated Hardware Threats

What is the Impact of Cybercrime / Cyber Attack?

Consequences of a cyber attack

Economic Costs

Theft of intellectual property, corporate information, disruption in trading, and the cost of repairing damaged systems.



Regulatory Costs

GDPR and other data breach laws mean that your organization could suffer from regulatory fines or sanctions as a result of cybercrimes.

Reputational Cost

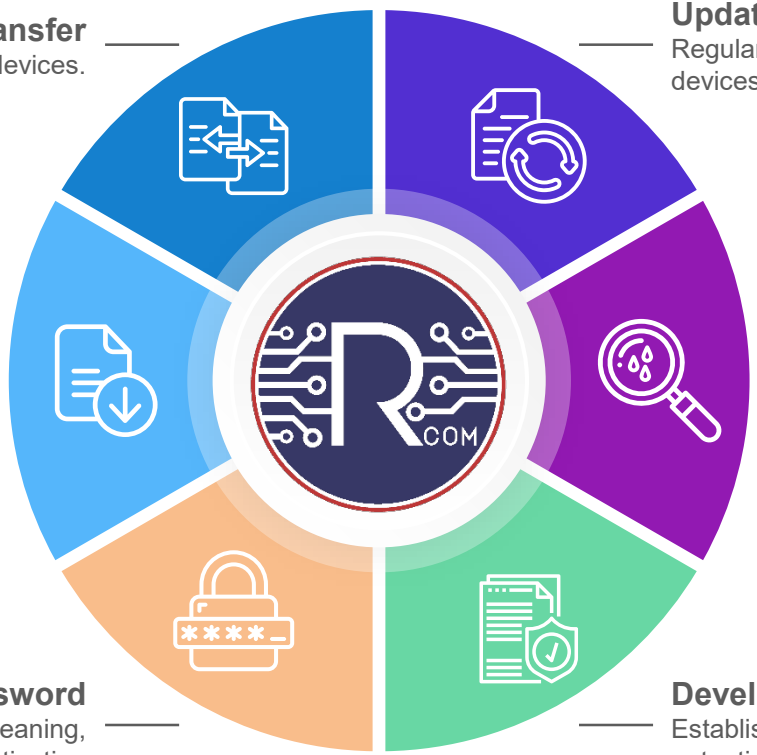
Loss of consumer trust, loss of current and future customers to competitors, and poor media coverage.

Cybersecurity Best Practices to Protect from Cyber Threats

How to Reduce the Risk of Cyber Attacks

Reduce Data Transfer
Keep sensitive data on personal devices.

Update Your Software
Regularly install the latest updates on your devices.



Download Carefully
Verify sources and avoid unnecessary downloads.

Monitor For Data Leaks
Quickly detect, respond, and stop any activity with software.

Improve Your Password
Use a string of symbols with no meaning, regularly update, and Multi Factor Authentication

Develop a Breach Response Plan
Establish a formal plan to manage and contain potential damage.

Cyber Security Checklist

- **Install anti-malware and antivirus protection**
  to safeguard against viruses that can corrupt your system and destroy your data.
- **Stay up-to-date with device and software updates**
  to eliminate bugs and security vulnerabilities.
- **Change default credentials**
  to prevent unauthorized and malicious access.
- **Use strong passwords and implement MFA (2FA)**
  that can't be easily cracked!
- **Use a password manager**
  so, you can use different password without having to remember them all.
- **Be cautious of freeware**
  by first ensuring apps are reputable and safe.
- **Avoid phishing emails and bad links**
  by deleting suspicious messages from unknown senders.
- **Use search engines to find websites**
  to avoid visiting malicious websites due to URL misspellings.

Your business is unique

and your security solution should be too.

Cyber and Network Security is not a DIY project. You need an IT Service and Security Partner that will be a Police Department and not a Fire Department. If you wait until something breaks, it's too late.

RCOM is an authority in all of these services and will customize your security plan to meet your individual needs.

Thank You for your time today
now let's open the floor to Q&A