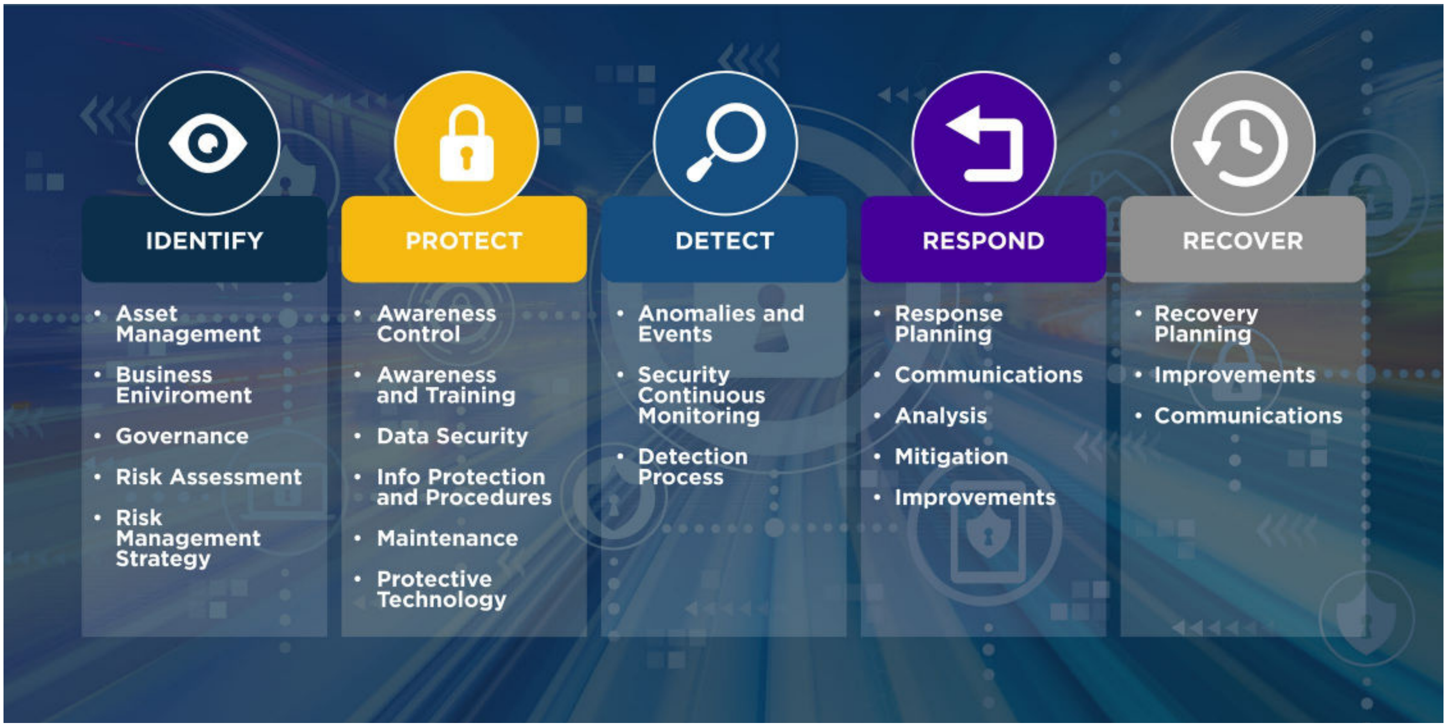
Help Protect the Integrity and Functionality of Your Data, Networks, and Systems

Why You Should Look at Reviewing the Security/Cybersecurity Readiness of Your Business

Why security is important. How reliant is an organization on information and data? Customer bases. Order processing. Employee files. Proprietary systems/data. Day-to-day functioning. Organizations of every size, scope, industry, and endeavor rely on their data integrity and ability to work with it — from managing a bank's payroll to protecting a school's student information to life-critical patient information. Every day you read about organizations being breached in the news. Threats are becoming more sophisticated and frequent. The solutions range from small, easy to embrace ideas, like providing employee training, to extremely complex concepts, like systems that learn to screen for files that behave in certain ways. There's no "fix in a box". Cybersecurity requires an overarching plan, dedication, and frequent revisiting.

53% of connected medical devices and other healthcare IoT devices have at least one unaddressed critical vulnerability.
— **HIPAA** Journal

NIST Framework: Identify, Protect, Detect, Respond, and Recover defined by the National Institute of Standards and Technology agency, provides a good overview of the approach all organizations should take.



IDENTIFY

- Asset Management
- Business Eniviroment
- Governance
- Risk Assessment
- Risk Management Strategy

PROTECT

- Awareness Control
- Awareness and Training
- Data Security
- Info Protection and Procedures
- Maintenance
- Protective Technology

DETECT

- Anomalies and Events
- Security Continuous Monitoring
- Detection Process

RESPOND

- Response Planning
- Communications
- Analysis
- Mitigation
- Improvements

RECOVER

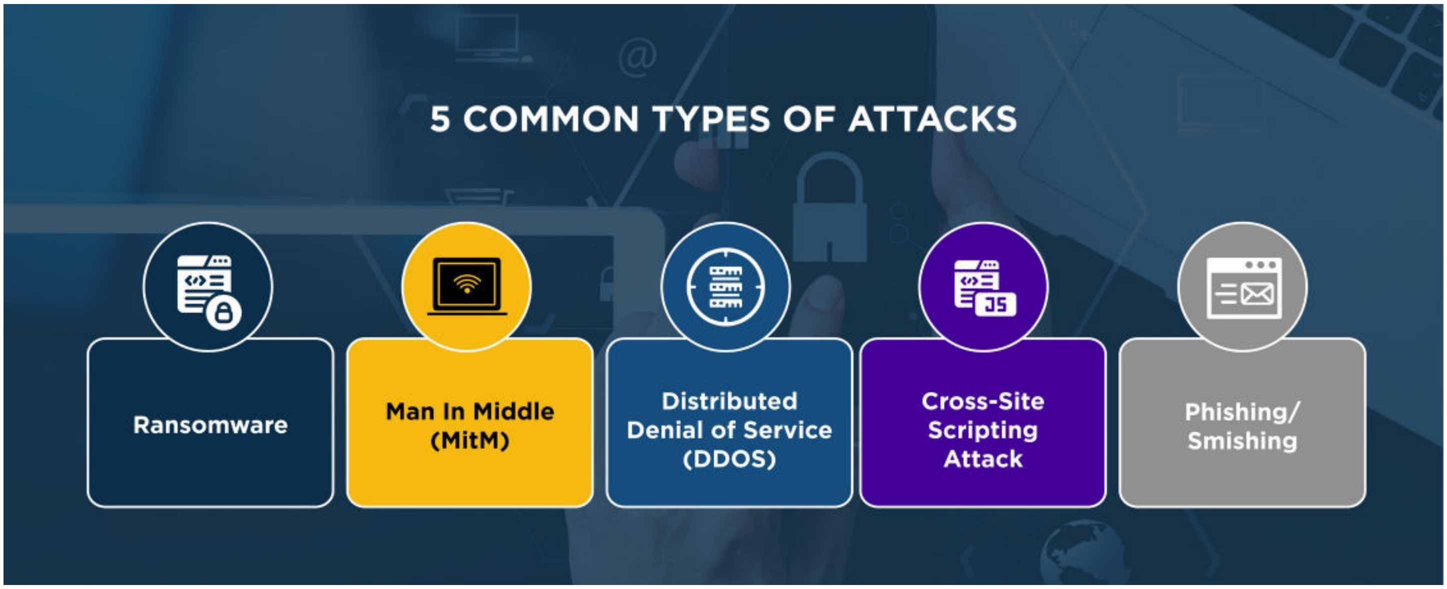
- Recovery Planning
- Improvements
- Communications

Defining the attack threat surface is a fancy way of saying identify the places where you're vulnerable. To reduce your risk, you reduce the threat surface. Some security experts emphasize an approach of global protection, while others segment the attack surface to minimize the impact of an eventual attack, and avoid organization-wide downtime.

Internal Threats. Some studies find that as many as 90% of threats come from within an organization, mostly from human error or carelessness, but also from malicious employees intending to disrupt operations or steal information. Organizations are encouraged to train their employees to be aware of everything from identifying potential incursions through emails/texts to controlling the devices that attach to the network and sites employees visit on the internet.

External Threats come from all over the world, exploits are even bought and sold on the dark web. Attacks can be targeted, or generalized in nature. They can be extremely aggressive and disruptive or be more subtle, scraping information over time. An attack can stop your organization in its tracks locking you out of important data, compromising infrastructure, or can lead to sensitive/proprietary information being lost or leveraged for illegal capital gain.

5 Common Types of Attacks


5 COMMON TYPES OF ATTACKS
Ransomware
Man In Middle (MitM)
Distributed Denial of Service (DDOS)
Cross-Site Scripting Attack
Phishing/ Smishing

Ransomware. System files are encrypted with a costly payment request to allow the attack to regain access to their files.

Man in the Middle (MitM). Information is caught while being transmitted on the Internet, the hackers will attempt to "sniff" and study the information to see if it can help them breach the system.

Distributed Denial of Service (DDOS). Occurs when more requests are sent to a target server than it can handle, effectively crashing it so it's unusable. These attacks can be coordinated and last for an extended period of time.

Cross-Site Scripting Attack. This occurs when JavaScript is used to exploit a web application, these attacks can be quite severe and provide a great deal of information to the hacker.

Phishing/Smishing. These attacks fall under the category of social engineering, a hacker sends a webpage URL that looks the same as the legitimate website, tricking the user into submitting their credentials which the hacker can use to gain access to the system.

Known Vulnerabilities, Testing for Weaknesses, and Behavior Profiling. When vulnerabilities and exploits are found, solution providers, including antivirus developers, will provide patches, profiles, and updates to address them. This relies on identifying a problem, finding a solution, and updating it — which can take some time. Alternatively, there are professionals (and some amateur enthusiasts) who will probe to find problems and notify the organizations or developer affected. One of the newer ways that relies heavily on Artificial Intelligence/Machine Learning is to look at known threatening behaviors and flag new interactions that follow these same behaviors.

Invest in Results, Mitigate Damages. In the security game, they say it's not if you'll be hacked/breached, but when. Organizations need to be proactive and security-wise — the cost of being unprepared can be heavy with lost operation time, reputation, and the resources needed to recover. Overworked IT departments often don't have the knowledge, bandwidth, or ability to develop and oversee effective strategies — which is where we can help make a difference by leveraging our portfolio of Security providers.

Our team is always here to help you secure your business!