# An Introduction to Cyber Security, and the Top Threats Today

ARTICLE 10.22.21  DEAN DORTON

Technology, for everything wonderful it's brought into our lives, can be a double-edged sword.

True, it has advanced how businesses in virtually every industry operate, connecting the world in near real-time and bringing new levels of convenience to everyday lives. After all, who doesn't love instantly streaming anything you want on any device at any time?

But with the convenience of technology, and desire to continually boost connectivity to more users on more devices than ever before, comes opportunities for cyber criminals to strike. Add to that equation a global pandemic that forced many companies to go remote — often with minimal security measures in place — and you have the perfect storm that has created an even more fertile breeding ground for relentless cyber attacks.

Understanding the types of threats that lurk in the shadows of the internet is the first step in adopting a cyber security framework and best practices to suit your needs. Here we'll cover an introduction to cyber security that every organization, large or small, should know about to help mitigate risks.

## What Cyber Security Is And Why It Matters

In broad terms, cyber security refers to the methods, techniques, and practices of protecting internet-connected networks, devices, software applications, and the sensitive data that travels through them all from unauthorized access.

The bad actors behind these threats most commonly look to leverage the sensitive data and compromise systems for financial gains, with businesses either forced to pay or suffer the fallout from lost data.

Now, with the proliferation of the Internet of Things (IoT) and sharp increase in the number of users, devices, and software programs that businesses rely on day in and day out, cyber attacks are becoming more frequent and complex.

And while many high-profile companies have made recent headlines for being unable to protect their customers' sensitive information from breaches, small to medium size businesses remain particularly vulnerable. According to Accenture's Cost of Cybercrime Study, 43% of cyber attacks are aimed at small businesses, yet only 14% of those businesses stand prepared to defend themselves.

While putting a cyber security plan in place is the most proactive way to mitigate the risk of attacks, there is no one single solution to prevent all attacks. But with strategic measures you can **increase real-time visibility** across your network and devices, and **improve your team's ability to react** in the event a breach occurs. The quicker you're able to combat an incident, the better it is for your productivity and bottom line. Perhaps more importantly, the better it is for

your reputation and the trust your customers have with you to keep their information secure.

## Types of Cyber Security

Cyber security is constantly evolving, and consists of a growing set of processes, risk management approaches, technologies, and best practices. Here are the basics on a few of the most common types of cyber security that businesses are focusing on and deploying today.

- **Network Security:** Helps to protect internal traffic by controlling incoming and outgoing connections to prevent threats from accessing or spreading across the network. Important layers of network security can include antivirus programs, antispyware, and a network firewall that can control traffic based on security settings and permissions.
- **Application Security:** Applications these days are more accessible than ever over various networks, and therefore can be especially vulnerable to attacks. Measures like requiring a strong user password, antivirus programs, firewalls, and encryption services are most effective when implemented before the application is deployed.
- **Information Security:** Often confused with cyber security, “InfoSec” is a crucial part of overall cyber security that refers to the processes and tools designed to protect sensitive information from modification, disruption, and destruction. The three primary tenets of InfoSec include confidentiality, integrity, and availability.
- **Cloud Security:** Cloud models allow for more convenience and an “always on” connectivity that requires more advanced considerations to keep them safe. Cloud security measures focus on building and hosting secure applications, enabling data recovery in case of loss, storage and network protections against malicious attacks, identity and access management (IAM), and reducing human error that can result in data leaks.
- **Data Loss Prevention (DLP):** Data loss prevention focuses on three common pain points experienced by organizations of all sizes: personal information protection, intellectual property (IP) protection, and data visibility. DLP software tools monitor and control endpoints, filter data streams on networks, and protect data while at rest, in motion, and in use. Once a breach is detected, DLPs alert IT professionals and provide encryption to prevent end users from maliciously or accidentally putting sensitive data at risk.
- **End User Education:** Research indicates that 90% of cyber claims stem from some type of human error or behavior. It’s a major point of weakness that even hiring a qualified technology partner to manage security won’t protect an organization from. One key and cost-effective first step to securing sensitive data is to implement cyber security training for internal teams to understand their role in device security, network responsibilities, and how to identify signs of malicious activity.

## Threats and Types of Cyber Security Attacks

The battle against cyber crime is a multi-front war. As technologies continue to advance, so do the cyber criminals, devising new threats and attacks that can be detrimental to businesses every day. As a starting point, these are a few of the more common threats that a comprehensive cyber security plan can help identify and provide safeguards against.

- **Social engineering:** A manipulation technique built around how people think or act to exploit human error that can lure unsuspecting users to expose data, spread malware infections, or provide access to restricted platforms.
- **Phishing:** This type of social engineering is particularly effective because the message or email appears to come from a credible source. Attackers are seeking to install malware or access sensitive information like credit card details and login credentials.
- **Malware:** One of the most common types of attacks, “malicious software” gets installed into a system when a user clicks a dangerous link or email. Once inside, it can block access, damage systems or devices, and gather critical data. Types of malware include spyware, viruses, worms, and **ransomware**, where an attacker locks or encrypts the victim’s data until paid.
- **Denial of Service:** These attacks are meant to flood servers or networks with massive amounts of traffic to deny fulfilling legitimate requests. When attacks compromise multiple devices to launch attacks on the target it’s known as **Distributed Denial of Service (DDoS)**.

- **Advanced Persistent Threats:** ATPs use continuous, sophisticated techniques to gain access to a system, allowing the attacker to remain there for a prolonged period of time. While a more common threat to larger organizations, cyber criminals are targeting smaller businesses that are part of a supply chain as a stepping stone to reach their ultimate goal.

## Maintaining Vigilance and Action

Some organizations in certain industries — like financial and healthcare as examples — are simply more vulnerable to cyber attacks based on the nature of the business. The more personal data that flows through their network, the more attractive they become as a target.

But in the wake of COVID and the exponential growth of remote workplaces in the past 20 months, businesses of all sizes and across industries need to be on guard.

An important first step to mitigating risks and safeguarding your valuable data — as well as your reputation with customers — is to assess your current cyber security stance. Connect with Dean Dorton for a cyber security assessment today.

*And for more insights and analysis on trends and cyber security solutions, be sure to subscribe to our blog.*