What Is Cybersecurity?

The practice of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

At least, that's what the dictionary says. Do you agree?

Over the years the term cybersecurity has been thrown around to the point where it is almost synonymous with terms like IT security or information security. It's kind of like saying every square is a rectangle, but not every rectangle is a square.

Every square IS a rectangle because a square is a quadrilateral with all four angles being right angles. Similarly, cybersecurity IS a part of the IT security umbrella, along with its counterparts, physical security and information security.

But not every rectangle is a square, since the criteria to qualify as a square means all sides must be the same length. The point is, not all IT security measures qualify as cybersecurity, as cybersecurity has its own distinct assets to protect.

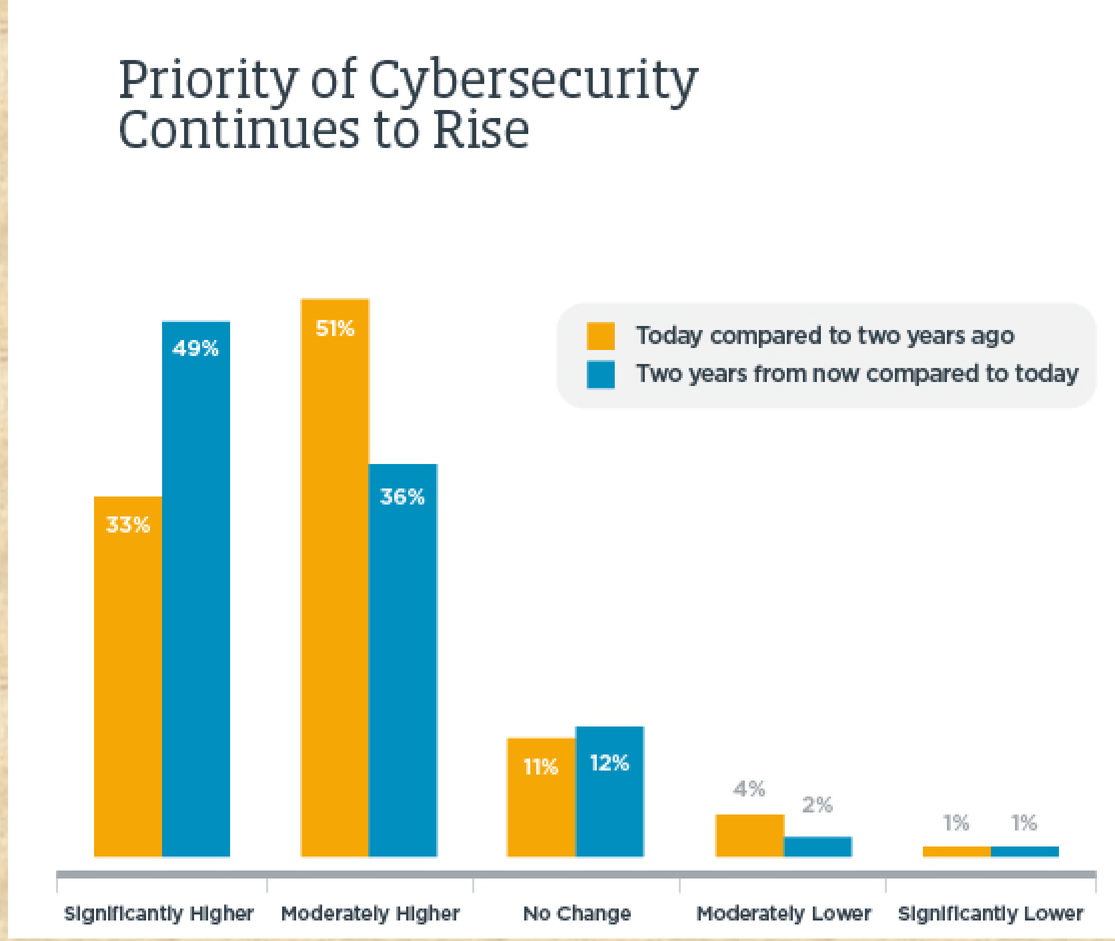
CompTIA's Chief Technology Evangelist, James Stanger says it best when he defines cybersecurity as "focusing on protecting electronic assets – including internet, WAN and LAN resources – used to store and transmit that information."

Of course, the threat to these electronic assets are hackers who have malicious intent to steal proprietary data and information via data breaches. Thus, it would seem the fully realized definition should include an evolving set of cybersecurity tools designed to protect confidential data from unauthorized access. To do so, it's necessary to consider how people, processes and technology all play equally important roles in keeping information safe.

Why Is Cybersecurity Important?

One of the many advantages to living in a world where every device is connected is convenience. It's incredibly easy to conduct work, manage your social calendar, shop and make appointments from your smartphone or device. That's why it's become second nature to many of us.

But, of course, the convenience of connected data also means threats from bad actors can do a lot of damage. Cybersecurity initiatives are essential to protecting our data and thus, our way of life.



Types of Cybersecurity

Cybersecurity can be categorized into five distinct types:

Critical infrastructure security

Application security

Network security

Cloud security

Internet of Things (IoT) security

Processes

When employees outside of the IT department are trained, IT pros can focus on process. The processes by which cybersecurity professionals go about protecting confidential data are multi-faceted. In short, these IT pros are tasked with detecting and identifying threats, protecting information and responding to incidents as well as recovering from them.

Putting processes into place not only ensures each of these buckets are being continuously monitored, but if cybersecurity attacks happen, referencing a well-documented process can save your company time, money and the trust of your most valuable asset – your customers.

The National Institute of Standards and Technology (NIST) under the U.S. Commerce Department has developed the Cybersecurity Framework for private-sector companies to use as a guide in creating their own best practices. The standards were compiled by NIST after former U.S. President Barack Obama signed an executive order in 2014. It's a great resource to use as you work to combat your cybersecurity risk.

Technology

Once you have frameworks and processes in place, it's time to think about the tools you have at your disposal to start implementation.

Technology has a dual meaning when it comes to your toolbox:

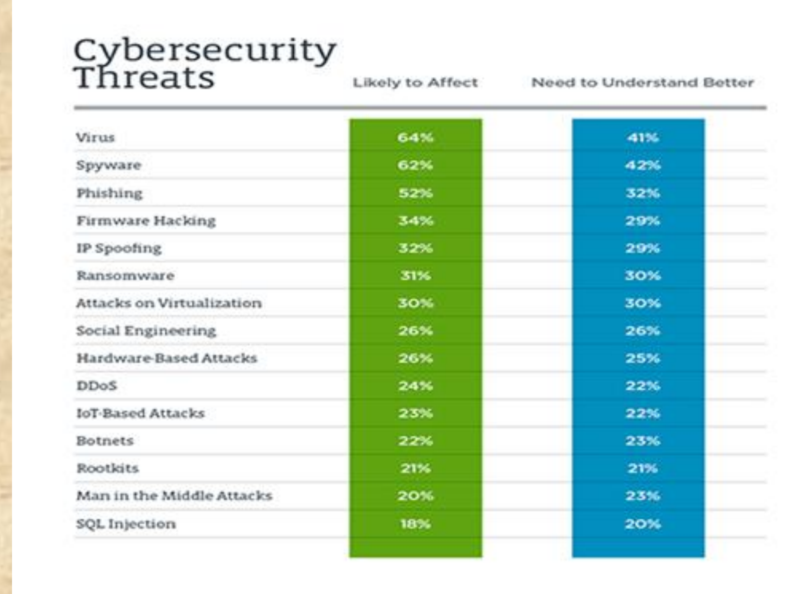
The technology you'll use to prevent and combat cybersecurity attacks, like DNS filtering, malware protection, antivirus software, firewalls and email security solutions.

The technology your data lives on that needs your protection, like computers, smart devices, routers, networks and the cloud.

Back in the day, cybersecurity initiatives focused on defensive measures inside the boundaries of traditional tech. But today, policies like Bring Your Own Device (BYOD) have blurred those lines and handed hackers a much broader realm to penetrate. Remembering cybersecurity basics like locking all of your doors, windows, elevators and skylights will keep you from joining the cyber-crime statistics.

Types of Cybersecurity Threats

Staying ahead of cybersecurity threats isn't an easy job. There's a long list of threats that IT pros pay attention to, but the problem is that the list keeps growing. Today, cyberattacks happen on the regular. While some attacks are small and easily contained, others quickly spiral out of control and wreak havoc. All cyberattacks require immediate attention and resolution.



Cybersecurity Threats

Cybersecurity Threats	Likely to Affect	Need to Understand Better
Virus	64%	41%
Spyware	62%	42%
Phishing	52%	32%
Firmware Hacking	34%	29%
IP Spoofing	32%	29%
Ransomware	31%	30%
Attacks on Virtualization	30%	30%
Social Engineering	26%	26%
Hardware-Based Attacks	26%	25%
DDoS	24%	22%
IoT-Based Attacks	23%	22%
Botnets	22%	23%
Rootkits	21%	21%
Man in the Middle Attacks	20%	23%
SQL Injection	18%	20%

Here are a few common cybersecurity threats that fall into both categories.

Malware

Malware is software that has been created to intentionally cause damage. Commonly known as a virus (among other things), malware can cause harm simply by opening the wrong attachment or clicking on the wrong link.

Ransomware

Ransomware is actually a type of malware. The difference here is that ransomware infects a network or steals confidential data and then demands a ransom (typically currency of some sort) in exchange for access to your systems.

Phishing Attacks

Phishing is just like it sounds. Hackers throw a line out there hoping that you'll bite, and when you do, they steal sensitive information like passwords, credit card numbers and more. Phishing attacks usually come in the form of emails that look legitimate and encourage you to reply.

Social Engineering

Social engineering involves malicious human interaction. This is a case of people outright lying and manipulating others to divulge personal information. Often, these people obtain information from social media profiles and posts.

Prof. Ashwini Haryan

Assistant Professor