Today's Cybersecurity Landscape

When it comes to cybersecurity, there's good news and bad news. The good news first: according to new research from CyberArk, the vast majority of IT professionals believe we're making real progress in the cyber security battle. That feeling of confidence may come in part from the fact that three out of four IT pros say they are doing a good job at keeping hackers from breaking into the network.

The bad news: businesses are still struggling to put best practices in place when it comes to security. Areas such as privileged access, third-party vendors, and even use of the cloud have weak security oversight.

All of this makes companies vulnerable to hackers, who take advantage of every means possible to infiltrate networks and collect data. Take the Yahoo breach, for example. Although details about the hack that compromised more than 500 million records are still being investigated, it appears that Yahoo's executives made customer convenience a higher priority than security. Now, personal information, including birth dates, addresses, passwords and even security questions and answers, are among the compromised data that has been shared or sold.

It's not just weak security measures that increase vulnerability to attack. Hackers take advantage of the proliferation of devices to find more ways to infiltrate the system. They use smartphones, tablets, and the many devices included in the Internet of Things as a way to spread malware. All too often, security for these devices is ignored, either by not adding security tools or not creating security policies to cover the devices.

What are the Biggest Cybersecurity Threats?

There may be no bigger threat to cybersecurity today than ransomware. Ransomware as an attack choice is skyrocketing, increasing more than 500 percent between 2015 and 2016, and the attacks are evolving at the same time. The days of paying a couple hundred in bitcoins to release encrypted data may soon be past. More frequently, hackers are only releasing part of the data upon payment, and asking for more payments to release the rest. The attacks are becoming more targeted as well. The healthcare industry is currently the favorite target for hackers, with reports of 20 data-loss incidents per day.

Even the FBI has taken notice of the rise in ransomware attacks. The agency recently released two separate public service announcements, one asking businesses to report ransomware attacks to law enforcement officials immediately, and the other warning against paying ransom,

while recommending companies have good data backup and disaster recovery mechanisms in place so they don't lose any down time or files.

In addition to ransomware, there are a number of other cybersecurity threat vectors and problems for IT departments to be aware of, including:

- Distributed denial of service (DDoS), attacks that overwhelm and take down websites
- Mobile malware, especially for Android
- Inside jobs that include both employee mistakes and malicious intent
- Social engineering, particularly spearphishing attacks and using social networking sites as an attack vector

How Can I Protect my Network and Data?

Good cybersecurity begins with an understanding of how to recognize security threats and the steps to take to avoid them. Understanding the cybersecurity landscape helps you see what types of threats are presenting the most risk today and how that will evolve into the risks of tomorrow. Training and education for employees will cut down on the accidental insider threat, as well as help your employees become more invested in protecting company data.

Your cybersecurity landscape is going to differ from your business neighbor's, and depends on factors like company size, industry, and your employees' security IQ. To protect your network and all of your data, a good place to start is with a Threat Sketch Risk Assessment. This helps you evaluate your company's threat landscape and provides you with the information you need to make an accurate risk assessment. Once you understand where your risks are, you'll be able to build a security system that best fits your needs.