**Unit 12 A Look into the Future of Cyber Security**

Cybersecurity has existed since the creation of the first computer virus in 1971.

That was the “creeper” virus, a harmless application designed to replicate and move from computer to computer.  New malware is created every day, however, by “threat actors” who attempt to develop new tools for often-nefarious purposes.

Cybersecurity professionals attempt to stop them, each investing to out-perform the other, in what has become a cat-and-mouse game.

In the decades sense, the sophistication on all sides in the game have increased.

“Cyberthreats have grown in scale and complexity; the attack surface – the breadth of exposed targets that an attacker might go after – has become exponentially larger with the birth of the Internet and now again with the birth of the Internet of Things,” said Eric Knapp, a chief engineer at Honeywell and expert in cybersecurity. “Meanwhile, the tools available to detect and prevent threats has likewise improved.”

Machine learning and AI are being used by both sides to continue this game of cat-and-mouse. Quantum computing will be next, exponentially elevating the capabilities of an attacker and a defender. So the cat and the mouse will keep getting better and faster, but the overall game isn’t going to change too much.

Here's what the future of cybersecurity will look like.

More ransomware threats

Ransomware has been slowly growing into a dominant (if not the dominant) cyberthreat for several years. Ransomware has become more prolific and potent for years. As a result, it’s also become extremely effective. There’s a direct financial benefit to the groups behind ransomware campaigns. Ransomware is now being incorporated into larger attack campaigns, where adversaries steal sensitive information before encrypting a target’s data, and they also attempt to prevent data recovery practices by preemptively targeting backup and recovery tools. That trend will continue.

USBs will be a more potent threat

USB devices are everywhere.  People are used to seeing them, using them and owning them.   Threat actors highly target USBs to penetrate industrial targets.  In our recent USB threat report, we found that 19%of the threats detected were designed to leverage USB removable media in some way. USB threats to industrials more than doubled to 59 percent. There’s a tendency for many people to underestimate ‘malware’.  To most laypeople, a ‘virus’ is the adware or spyware you are frustrated with on your personal computer.  But malware can be much more serious and much more dangerous, and in some cases in OT this can translate to loss of view, meaning operators are blind to the process, and can not properly monitor conditions. That is very dangerous in high-risk industrial environments. The malware can also cause loss of process, either directly damaging or stopping a process. In our latest USB threat report, we saw the amount of high-impact malware doubled.

Secure remote access

The recent shift to remote working is causing the need to guarantee security of remote access. Companies must rethink their security plans around a highly distributed infrastructure. Meanwhile, attackers are evolving their approach, finding ways to target employees who are working in isolation but still connected into the corporate network. In operational technology, the best-practices that have existed for decades have prepared the cybersecurity industry for keeping critical tasks completely and physically separated. For example, a critical remote worker might have a uni-purpose laptop that is only capable of performing a single task and won’t have access to email, social media, or any public network connections at all.

Increased automation

Technology to be able to perform efficient cybersecurity tasks. It’s simply the result of scale.  Successful cyber will always boil down to people – skilled human minds playing the role of either the cat or the mouse. But there are too many things to watch, too many threat variants (there are easily more than a billion viruses today), too many vectors, too many targets. That must be simplified. Today, we’re already using machine learning and artificial intelligence to help make sense of all that noise before it gets presented to human security professionals.

Computers have limitations, and attacks are aware of this.  It’s a very common tactic among hackers to create diversions, filling security analysts’ screens up with red herrings or maybe just bogus events.  Eventually even the best analysts, armed with the best tools, will get overwhelmed.  The cloud has helped a lot in this area – it’s improved the ability to scale and lowered the cost (making it feasible to use). Quantum computing will also play a major role, helping sift through complex scenarios and detect or predict even faint traces of a threat.

Ultimately, cybersecurity defense in depth strategy will not go away.  Organizations will never have one silver bullet to completely reduce the risk of a cyber-attack but rather multiple technologies and processes in place to help ensure those threats are minimized.