Predicting What 2022 Holds for Cybersecurity

by Emil Sayegh

Chief Executive Officer, Ntirety

Ntirety™

2021

was a fascinating and somewhat terrifying year for cybersecurity.

All our fears regarding cyber-threats have come true in one way or another. 2021 was tricky, as many organizations have been slow to adapt to the new security climate. Predictions aside, complacency is not an option if you plan to survive and thrive in 2022. Rest assured, the future of cybersecurity is bright, but it will come with its own set of challenges. We look forward into the future because the sooner we can start adapting strategy, policies, and technologies, the better off everyone will be in the long run. Predictions can be both exciting and terrifying at the same time, so please put on your seat belt and helmets.

2022 Cybersecurity Predictions

THE CYBERSECURITY TALENT DROUGHT WILL GET MUCH WORSE

The cybersecurity talent shortage that affects the industry is only going to get worse. At one point in 2021, there were 500,000 unfilled cybersecurity jobs in the U.S. That's a figure that is likely to increase due to the continued growth of ransomware, data breaches, and other cyberattacks.

Faced with this challenge, businesses will find it increasingly difficult to protect their networks and data. Services and specific technology partnerships will continue help fill and protect that which is sacred, but further help may be on the way from an unlikely place: artificial intelligence (AI). AI has the potential to detect malware on networks before it is spotted by employees. Along with machine learning, these technologies can better analyze vast quantities of data more quickly than humans, detecting sneaky issues such as phishing attacks, privilege escalations, data exfiltration, and insider threats.

2022
Cybersecurity
Predictions

SUPPLY CHAIN CYBERATTACKS WILL BE COMMODITIZED

In recent years, we have seen a significant increase in the number of cyberattacks targeting software supply chains. These attacks are particularly effective because they can take down an organization's entire software supply chain and services, resulting in massive business disruptions.

Unfortunately, we can expect these attacks to become even more common in 2022. Cybercriminals will realize that these supply chain attacks are an effective way to cause maximum disruption, and once inside the trusted gates, the hardest part of the hack job is already handled. These groups will commoditize these attacks as a result. We can expect this commoditization to lower the bar for entry by encouraging less skilled attackers to conduct software supply chain attacks.

2022 Cybersecurity Predictions

THE DEATH AND REBIRTH OF CYBER INSURANCE

Faced with a costly environment of escalating risks, the cyber insurance industry has seen many challenges in the past year and the premiums for coverage have skyrocketed. Even though many businesses are required to carry cyber insurance, these conditions are leading to companies no longer purchasing extensive policies. This market squeeze will certainly affect the cyber insurance industry itself.

We are going to see this happen, but we will also see a resurgence of cyber insurance as companies become more aware of the risks associated with data breaches and standardize on what it takes to attain coverage. Cyber-Insurance without Comprehensive Security, will become a non-starter.

Combined with a growing awareness of the risks associated with data breaches and cyber incidents, the market for cyber-insurance is starting to mature, and premiums will become prohibitively more expensive for companies that don't have a sound security strategy.

MORE SMART DEVICES, MORE RISK

It's inevitable -The Internet of Things is a continually growing trend that will bring about more cyberthreats. In 2022, we can expect to see even more cyberattacks due to the increased number of IoT devices. The proliferation of these often minimally protected devices increases the threat vectors through everyday devices. Hackers can attack through many vulnerable devices such as security cameras, smart TVs and DVRs in your home or workplace.

The Mirai Botnet was one such attack which took down several high-profile websites with a denial of-service (DDoS) attack. This botnet was made up of millions of hijacked IoT devices and attackers will always be looking for the maximum bang for their hacking buck.

2022 Cybersecurity Predictions

CYBERATTACKS WILL COST LIVES

The world is no stranger to the amount of damage hackers can cause. We have seen attacks on hospitals, transportation systems and even schools leaving hospitals paralyzed, cities without electricity and students' grades showing up as Fs. However, what many people have a hard time imagining are the effects of a hacker setting their sights on critical infrastructure like power plants or dams.

Threats will become all too real when an upcoming attack results in disruption and death. It's not a pretty picture, but the actions of world leaders have indicated that cybersecurity is the front line in a global cyberwar and casualties are just a logical hop away.

2022 Cybersecurity Predictions

SHTF EVENTS WILL PUT DISASTER RECOVERY INTO THE FOREFRONT AGAIN

Expect the unexpected. Seldom have three words carried so much weight. An improbable but all too real SHTF scenario is out there waiting in some company's destiny, but it doesn't have to go the way of painful recovery. You can't plan for everything, but you should plan for anything.

From cyber incidents to weather disruptions, to natural disasters of every type, major events will drive a resurging focus on enterprise disaster recovery (DR) in the year ahead. The cost of not thoroughly protecting these systems is higher than ever and the events experienced in the last year are the beginnings of a wake-up call for both businesses and governments around the world. The need to protect critical infrastructure and data is now at the forefront of every boardroom conversation and government policy.

2022 Cybersecurity Predictions

MACHINE LEARNING/AI TOOLS CONTINUE CHANGING THE GAME FOR CYBERSECURITY

Machine learning (ML) and artificial intelligence (AI) have already started to revolutionize cybersecurity, and their impact is only going to grow in 2022. These tools are making it possible for organizations to detect and respond to threats much more quickly and effectively than ever before. Security professionals can identify potential attacks more quickly than ever before with AI-powered dashboards. Meanwhile, machine learning tools can be used to detect ransomware in an image file before it's opened on a computer.

Cybersecurity teams will use ML and AI to automate the detection of attacks, understand the impact of a breach, and reduce fraud.

2022
Cybersecurity
Predictions

MORE CYBER CRIMINALS IN THE SLAMMER

Law enforcement agencies have stepped up their efforts to catch cyber criminals. While the biggest headlines seem to show that the perpetrators are never caught, many successful investigations have been resulting in prosecution. This increased trend is going to continue as law enforcement officials become even better at identifying and apprehending cybercriminals. That's good news for businesses and consumers alike, as cybercriminals will have a reduced ability to operate with impunity.

2022 Cybersecurity Predictions

TABLES WILL TURN: CYBER CRIME WILL HIT INTERNATIONAL COMPANIES IN CHINA AND RUSSIA

A recent major cybersecurity report found that four in five large international companies have been targeted by cybercrime in China and Russia. The sad part that 40% of companies that lose data or have a data breach, end up going out of business due to the cost and reputational damage. These companies have fallen victim to a wide variety of attacks, including malware, ransomware, and phishing.

As it turns out, nobody is immune to cyber threats and you shouldn't do business with criminals. Foreign nations have been dancing a perilous line of espionage and state-sponsorship of attacks on adversarial and strategic targets. The tables are going to turn on them at some point.

2022
Cybersecurity
Predictions

QUANTUM COMPUTING TO MAKE A DEBUT

This one has been building up for a while now, but this should finally be the year that quantum computing debuts in the cybersecurity world. We are talking about actual quantum computing, not the marketing type of quantum-like features.

The breakthrough will be small at first but expect to see products that can take advantage of the peculiar properties of quantum mechanics to do things like factor large numbers very quickly or break current cryptography within a few years. This could also present a serious challenge to today's security protocols and necessitate a wholesale rethinking of how we protect our data.

Quite a Year Ahead

There's a sense of foreboding in cybersecurity, especially when everything seems to be as safe as possible. Cybercriminals thrive on this false sense of security and subsequent complacency to do their worst. We must always be on guard, prepared for the worst. Cybercrime is rampant and the threats don't discriminate. This year alone, four in five large international companies have been targeted by cybercriminals - meaning that nobody's immune to the risk of a breach. Fortunately, there are ways we can protect ourselves against these risks: strong cybersecurity protections like firewalls, anti-virus software and intrusion detection systems; training for employees so they know how to avoid becoming victims themselves; and understanding what brings on data breaches. The best approach is to not only adopt a comprehensive security approach to every level of the IT stack, but also include all business processes in that approach.

Ntirety™