CYBER

CYBER RISK AND INSURANCE IN 2022

The cyber risk landscape has always been in motion, but the rate of change has accelerated during the pandemic and will likely remain volatile.

Lynn Ambrose MARCH 9, 2022

The pandemic has created new cyber vulnerabilities, heightened existing risk factors and accelerated the pace at which cybercriminals wreaked havoc on even the most secure systems. Undoubtedly, 2022 will see more of the same.

Many large organizations responded to heightened cyber threats by ramping up their security budgets and deploying state-of-the art security technology. Small and mid-size businesses with less sophistication and

Cybercriminals had a banner year in 2021. According to Check Point Research, cyberattacks increased 50% in 2021 as compared with 2020, with each organization facing an average of 925 attacks per week.

With large numbers of employees working from home and using their personal devices for business purposes, corporate networks were left vulnerable to the often-inadequate security practices of individual employees. According to security company CrowdStrike in their *2021 Global Treat Report,* this created a "feeding frenzy for cyber predators spurred on by the windfall of easy access to sensitive data and networks."

Phishing and ransomware were far and away the primary attack vectors, affecting both large and small businesses. Phishing attacks increased in number and sophistication as "fear, concern and curiosity surrounding COVID-19 provided the perfect cover for a record-setting increase in social engineering attacks," according to CrowdStrike. The *Human Hacking* report published by SlashNext Threat Labs data shows phishing attacks rose 51% in 2021 as compared with 2020.

Successful phishing campaigns often resulted in ransomware attacks. Ransomware is not a new cybersecurity threat, but it is one that cybercriminals have learned to use with far more devastating effect in recent years. Since the beginning of the pandemic, ransomware claims have increased four-fold. The average ransom demand increased about 900% as cybercriminals employed increasingly sophisticated and damaging tactics, techniques and procedures. One notable 2021 ransomware attack targeting pipeline operator Colonial Pipeline resulted in $4.4 million being paid to a Russian cyber gang.

In addition to the cost of paying the criminals, ransomware attacks also can cause downtime and business interruption losses. A 2020 attack on the University of Vermont Medical Center, for example, cost the hospital an estimated $50 million, mostly from lost revenue.

Many ransomware attacks are directed at supply chains. A single supply chain attack can hit numerous organizations, providing cybercriminals the ability to use a single intrusion to attack multiple targets. Cybercriminals often use smaller, more vulnerable companies in a supply chain to gain access to larger, better-defended companies.

One of the most widespread and sophisticated supply chain attacks targeted SolarWinds, a major information technology firm. SolarWinds unknowingly sent software updates to its customers including U.S. government agencies such as the Department of Homeland Security, the State Department, the Department of Energy, the National Nuclear Security Administration and the Treasury that was tainted with code that left them vulnerable to hackers. More than 18,000 organizations—both public and private—were affected.

Increased losses sparked higher prices and more restrictive underwriting criteria in the cyber insurance market. Prior to 2020, rates were held in check by competition as the cyber insurance market grew and matured. Additionally, underwriting results were generally favorable, which attracted capacity to the line of

quotes for the same piece of business varying wildly from underwriter to underwriter, all of whom are underwriting from the same submission.

In addition to raising premiums, underwriters tightened criteria and increased their scrutiny of network security protocols. Carriers also reduced capacity on individual risks and on their aggregate portfolio exposures.

Cyber risk management and insurance in 2022 and beyond

Many of the risk and insurance trends seen in 2021 are likely to continue through 2022. Network security at many organizations will continue to be under stress as employees continue to work from home, often using their own devices and security software. More than 50% of corporate executives surveyed by PwC for its *2022 Global Digital Trust Insights Survey* expect a sharp increase in cyber incidents in 2022.

Determined cybercriminals can defeat even the most advanced network security. However, business owners and their IT professionals can take simple and effective steps to deter criminals. Hackers look for poorly secured systems and often pass by better-guarded networks. According to PwC, “many of the breaches we’re seeing are still preventable with sound cyber practices and strong controls.”

Foremost to effective cybersecurity is an organization-wide security culture. Cybersecurity is not strictly an IT function—people, more than technology, make an organization secure. Cybersecurity culture must be driven from the C-suite and reinforced by communication, training and incentives for good cyber hygiene. Awareness and education help instill good cyber safety habits and reinforce what employees should and shouldn’t click on, download or explore.

From a technology perspective, multi-factor authentication on all business-critical systems is an effective, inexpensive way to boost security. In addition to the conventional username and password, other identifying information is required such as a personal identification number (PIN) or a specific keystroke pattern. Some experts are advocating password-less authentication—dispensing with passwords altogether in favor of alternatives such as requiring users to input a code that is either emailed or sent via text message.

Ransomware attacks—which are low-risk but high-return for cybercriminals—will continue to be one of the most common types of malicious cyber events. Organizations need to increasingly focus on backing up data and keeping those backups as secure as possible. Good cyber hygiene may deter attacks, but, once an attack occurs, secure backups are essential.

An information security architecture known as Zero Trust has grown in popularity in recent years. A Zero Trust approach uses security protocols and technologies designed to limit an attacker’s ability to move within or between systems to reach critical parts of the network. Commercial Zero Trust security solutions

environment and are attuned to underwriter cybersecurity preferences and demands. They thoroughly understand their clients' cyber exposures and security posture and can find the best fit in a market where coverage terms and prices can vary wildly from underwriter to underwriter and even from day to day.

See also: Quest for Reliable Cyber Security

The "next normal" of cyber risk and insurance

The future cyber risk landscape will be shaped by post-pandemic social, political, economic and technological forces and informed by the lessons learned by both attackers and defenders during the present unsettled environment. The cyber risk landscape has always been in motion, but the rate of change has accelerated during the pandemic and will likely remain volatile even as the COVID-19 threat recedes.

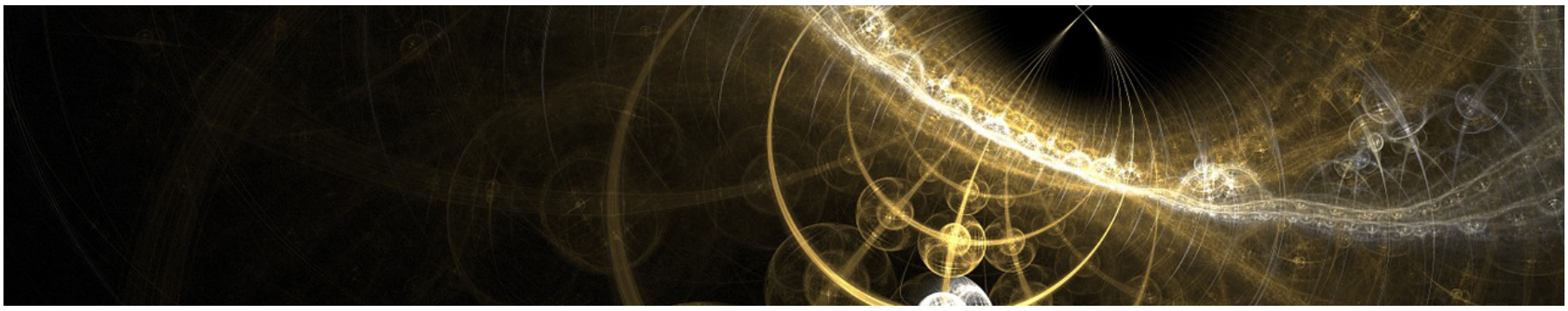
The cyber insurance market will continue to respond to a changing threat landscape, but also will be shaped by business, economic and regulatory forces. It also will respond to the internal demands of a still-young line of business as it matures. Working with knowledgeable and creative brokers who can navigate a chaotic marketplace, even comparatively small organizations will be able to deploy a risk management and insurance strategy that will contribute to growth and stability in a changed—and changing—environment.

Lynn Ambrose

Lynn Ambrose is vice president of The Plexus Groupe.

READ MORE

Recent macroeconomic events involving supply chain slowdowns, flexible work arrangements and rising inflation have paved the way for a possible uptick in crime.



THE CHALLENGE OF QUANTUM RESILIENCE

By **Vaibhav Uttekar**

Quantum computing, in the wrong hands, could create a multitude of digital risks, including advanced cyberattacks -- a significant problem for the insurance industry.

THE WEAK POINT IN CYBER SECURITY

By **Joseph Carson**

The best place to start is by securing a well-known defensive weak point: privileged access that has administrator-level powers.

IS INSURTECH OVER?

By **Paul Carroll**

Stock prices for marquee names have plunged, and venture capitalists are raising red flags about inflation and possible recession. But don't despair.

AUTO INSURANCE IN THE HYPERCONNECTED WORLD

1

Telematics is becoming a necessary capability for dealing with the future of insurance, especially in auto, and capabilities will only grow from here.

HOW IOT SHIFTS INSURANCE'S PARADIGM

2

Traditional discussions of react, repair and replace are changing to predict, prevent and protect. Part of this transition has been supported by the IoT.

IDENTITY MANAGEMENT: THE FUTURE OF MARKETING

3

Identity management involves reconciling what you know about an individual with real-time behavioral data, specifically actions that signal purchasing intent.

---

arrangements and rising inflation have paved the way for a possible uptick in crime.

5

PROPERTY UNDERWRITING FOR EXTREME WEATHER

6

Insurers have massive databases from simulation models and satellites when it comes to weather and climate. The problem is figuring out how to use them to their full...

ITL RECOMMENDS

HOW TO STOP ANNOYING YOUR CUSTOMERS

WHY ARE WE STILL TALKING ABOUT DIGITAL TRANSFORMATION?

By **Insurance Thought Leadership**, **ClarionDoor**

A SEVEN YEAR ITCH – CHANGES IN INSURERS' STRATEGIC PRIORITIES DEFINED BY THREE DIGITAL ERAS OVER SEVEN YEARS

By **ITL Partner: Majesco**

TECHNOLOGY IS THE SOLUTION -- AND THE PROBLEM

THE FUTURE OF WORK

About

Contact Us

Privacy Policy

Terms of Use

EMAIL ADDRESS

THIS WEBSITE USES COOKIES TO GIVE YOU THE BEST POSSIBLE EXPERIENCE

By clicking the OK button, you agree to us doing so.

OK