Cyber Security State of Tech in 2022

The Coronavirus pandemic accelerated technology adoption in ways thought unimaginable just a few short years ago. But in the background and often without much fanfare, cybercrime grew far worse. Threat actors continued their work – often backed by millions of dollars from hostile foreign governments – to penetrate networks and wreak havoc on digital infrastructures.

Our previous whitepaper revealed why cyber security is the biggest threat facing businesses today. In this document, we will share the state of cyber security tech in 2022 and discuss the near-term future as well.

What Trends Emerged in 2021?

The year 2021 brought about some noticeable trends in tech and how cyber security has fared so far. These trends include:

Remote work

For decades, remote work was a niche part of the economy: freelancers and virtual assistants completing a narrow set of tasks for businesses. But when offices began shutting down in March of 2020, organizations across the globe quickly adopted the model. Fully remote and hybrid work routines became common in virtually every industry.

But as with many emergency situations, the lack of preparation and thoughtful implementation has left security gaps. That includes things like unsecured wireless networks, misconfigured VPNs, unpatched and unmonitored "bring your own device" systems, and a lack of cyber security training and testing.

According to IBM and Ponemon Institute research, the shift to remote work has resulted in a spike in costly data breaches. Their analysis indicates that breaches related to remote work cost $1 million more on average ($4.96 million vs $3.89 million). Cybersecurity Ventures found that the number of complaints received by the Internet Crime Complaint Center (IC3) – an arm of the FBI – increased by 300% during the global transition to remote work.

Passwordless Authentication

Passwords are the preferred form of security for most modern systems. But memorizing dozens of unique, complex passwords isn't exactly easy. Security Boulevard states that 20-50% of all helpdesk tickets are for password resets every year. To reduce frustration, employees adopt bad habits - creating the simplest passwords possible and reusing them frequently.

Cybercriminals prey on easy-to-guess credentials, iterating over billions of possible combinations using custom software. Each data point they have (prior passwords, personal information about the victim, etc.) makes it easier for them to break in.

Although not an entirely new concept, 2021 saw the emergence of passwordless authentication to protect digital assets. There are a variety of ways that a person can demonstrate their identity, such as:

Each of these methods offers pros and cons, so IT leadership should consider which tools provide the best framework for strong, scalable security. Regardless of the method selected, wider adoption of passwordless authentication is a very welcome development.

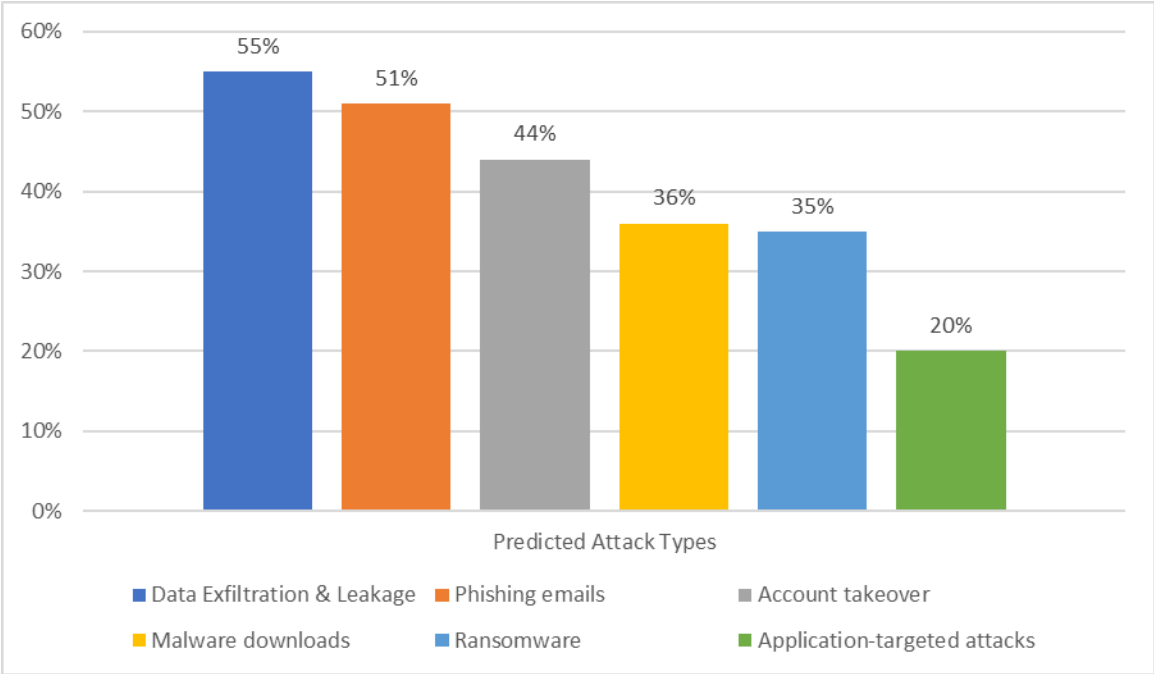
Evolving Cyberattacks

As the pandemic met unplanned and non-resilient digital security measures, 2021 became a busy year for cybersecurity teams. CNET reported that data breaches spiked 68% in 2021, reaching an all-time high. In fact, approximately 85% of businesses report experiencing a cyber attack in 2021.

The Identity Theft Resource Center's (ITRC) 2021 Data Breach Report recorded 1,862 data breaches in 2021 – surpassing the previous record of 1,506 set in 2017.

When IT professionals are polled, the results are incredibly consistent: successful attacks and attack attempts are predicted to increase year after year, with the leading attack types being data exfiltration/leakage and phishing emails.

Where do IT professionals see an increase in cyber attacks and attack attempts following the COVID-19 pandemic?

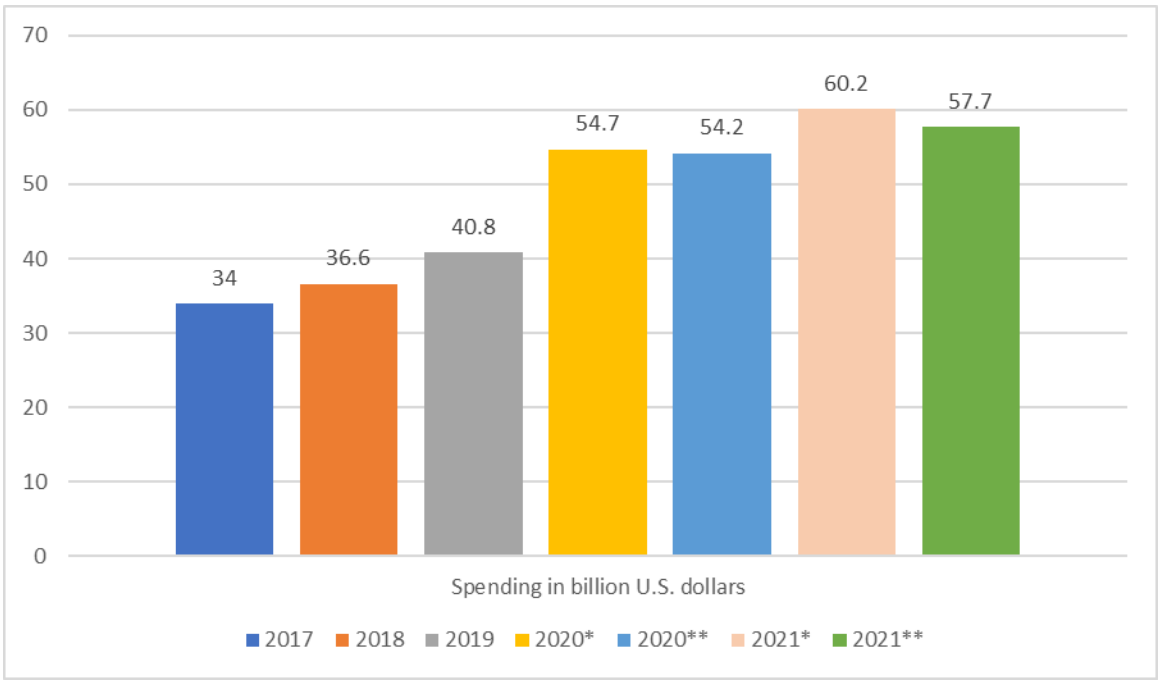


Source: Statista July 2021 Worldwide Study – 450 IT Security Professionals

Cyber Security Spending

Cyber security spending worldwide, according to Statista, may have exceeded $60.2 billion in 2021, surpassing the prior record of approximately 54 billion dollars, set in 2020. As we approach the end of 2022, the exact picture for spending in 2020 and 2021 should become clearer.

Worldwide cyber security spending from 2017 to 2021



*Forecast. Best-case scenario
**Forecast. Worst-case scenario
Source: Statista January 2021 Worldwide Study

Interestingly, the ITRC report pointed out that the *number of people* affected by data breaches actually dropped by 5% in 2021 to roughly 294 million. The reason behind the drop? In the pandemic and post-pandemic era, there have been proportionally more attacks on small and mid-sized businesses because they are easier to compromise.

Notable Cyberattacks in 2021

LATE JAN 2021

Company: 4th largest wireless carrier in US
How did it happen? Employees tricked into downloading malware
Impact: Perpetrators had unrestricted access to 276 customer names, addresses, phone numbers, billing plans, and PINs.

EARLY JUNE 2021

Company: World's largest meat processor
How did it happen? Ransomware attack
Impact: All of JBS' U.S. beef plants were closed temporarily. The extortionists were paid $11 million dollars

EARLY JAN 2021

Company: Internet of Things (IoT) and IT vendor
How did it happen? Unauthorized access by an employee via a third-party cloud provider
Impact: "Catastrophic" event that impacted stock prices and spurred a protracted legal battle

MAY 2021

Company: One of the largest refined oil pipeline companies in the U.S.
How did it happen? Attackers guessed a single password which was not protected by Two-Factor Authentication
Impact: The attack halted all pipeline operations for six days, impacting businesses nation-wide

JULY 2021

Company: IT software firm
How did it happen? Two serious security flaws in Kaseya's software
Impact: The attack affected the operations of 1,500 businesses on 5 different continents

What is the Prognosis for 2022?

In a single word, uncertain. Businesses are still adapting to the "new normal" but still not investing the time and resources necessary to protect their digital infrastructure and comply with emerging regulations.

What are Envision's predictions for 2022 and beyond?

An Increase in Extortion Events

2021 saw ransomware threats triple in the US, and targeted attacks spread worldwide. In response, President Biden made cyber security a key element of the Department of Homeland Security's mission.

Simultaneously, organizations are adding far more third-party providers to their technology stack, including cloud-based Software-as-a-Service (SaaS) platforms. That means cyberincidents may be caused by a "weak link" in the vendor network and wholly outside of the victim company's control.

Yet even when there is no internal cause for a successful attack, the fallout is the same: lost revenue, lawsuits, and a damaged reputation.

We expect 2022 to be a turning point year in the war against extortion events. The most successful companies will choose a comprehensive approach, adopting zero trust principles, implementing 24/7 monitoring, purchasing sufficient cyber liability insurance policies, and preparing detailed incident response plans.

By staying current on technology trends, these "best prepared" outfits will gain a measurable advantage over their competition, whether or not they are ever breached.

More Digital Attacks on Digital Supply Chains

The attacks against Colonial Pipeline and JBS Foods demonstrated how lucrative supply chain attacks can be. Bad actors and rogue states can get rich and devastate entire industries, with rippling effects through the entire economy. The problem is only going to get worse. Gartner predicts that 45% of organizations worldwide will suffer cyberattacks on their supply chains by 2025.

Phishing Scams Will Continue

If ransomware is the driver of significant cybercriminal operations, then phishing scams are riding shotgun. People are extremely trusting by nature and sincerely want to help those in need. But those good qualities can lead to manipulation. A single mistake – clicking a link or opening an attachment – can expose access to systems and data.

There's no indication that the volume of phishing scams will decrease. And without a national focus on cyber security training and testing, phishing will continue to net billions of dollars for crooks.

Vendor Consolidation

As corporations attempt to simplify their architecture while improving their defenses, the trend of security vendors merging will accelerate. Existing security platforms will gain new capabilities and enhanced features.

While having a "single point of failure" is always a risk, reducing the complex web of partners and improving performance is beneficial overall.

More Insider Threats

2022 has been called the year of the Great Resignation. Consequently, there has been a spike in insider threats as people intentionally or unintentionally carry sensitive data out of their former employers. Far scarier is the possibility of disgruntled employees being recruited by criminals to steal data or dismantle systems.

2022 should be the year of vigilant monitoring to protect financial assets, data, and intellectual property. Whether it is or not remains to be seen.

Privacy Legislation Gains More Grounds

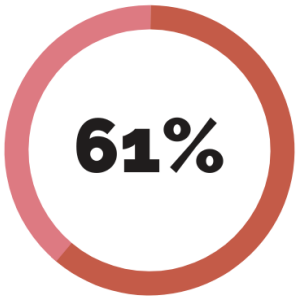
Whenever a splashy data breach is covered by the media, consumers ask about the type of information that is being collected and stored. As a result, we could see new privacy laws inspired by the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA).

The Rise of XDR

As cybercriminals proliferate in the tech ecosystem, CTOs and other Senior Managers are seeking new ways to prevent data breaches. Initially, corporations deployed Endpoint Detection and Response (EDR) to actively monitor and respond to threats. EDR helps companies log endpoint data and alerts on suspicious behavior. However, there are several limitations to EDR.

EDR is heavily dependent on data collection agents, which are designed to be lightweight, but that limits their visibility. Not all IoT devices can support EDR agents, leaving them susceptible to attacks. And because EDR only monitors endpoints, it does nothing to protect cloud platforms and network hardware from attack.

In 2020, TrendMicro found that 61% of organizations manually aggregate data from different security solutions.



This approach limits defensive capabilities and slows incident response times.

Gartner elaborated by saying that EDR platforms “no longer address the nature of modern threats as [they] no longer practical to focus on achieving 100% prevention and protection.” In 2022 and beyond, organizations must re-assess and select more comprehensive security solutions.

Extended Detection and Response (XDR) is a cross-functional, hybrid security tool that provides robust detection and response that extends beyond endpoints. XDR enables IT analysts to establish control over their systems.

Because XDR is unified in its operations, it allows straightforward implementation across endpoints, email, cloud platforms, and other solutions. XDR gives CSOs and their IT departments an eagle-eyed view of cybersecurity performance, detecting and responding to threats in real time.

The Modern Cybercriminal

When you hear the term “cybercriminal”, you might picture lone criminals operating out of their basements. But more often than not, they’re highly skilled professionals who work for sophisticated crime syndicates.

Cybercrime organizations conduct themselves like legitimate businesses. Caleb Barlow, Head of Threat Intelligence for IBM Security, noted, *“We can see the discipline they have, we can see that they are active during office hours, they take the weekends off, they work regular hours, and they take holidays.”*

At the top of most outfits is a CEO that develops strategic plans. Beneath them are project managers that oversee specific cyberattacks. Like most organizations, they map out their activities and assign tasks to achieve monthly, quarterly, and yearly goals.

Playing nice with these groups doesn’t always work. According to a survey by Cybereason, 80% of extorted businesses that pay a ransom are attacked a second time. 46% of those companies believe that the second attack was caused by the same people.

Cyber Security Solutions

As a trusted advisor, Envision guides businesses to cyber security solutions. While no “perfect” strategies exist, you can reduce the likelihood of an attack by deploying the following measures:

More Artificial Intelligence

Studies suggest that 85% of data breaches are caused by human error. While advances in artificial intelligence related to gaming, robotics, and autonomous vehicles are well-known, AI is making large strides in preventing cyber threats.

AI can provide faster threat prediction and identification. Machine learning can be designed to conduct predictive analyses and leverage complex algorithms to detect malware. It can also automate lengthy validation processes to differentiate between good and bad actors. AI is also crucial in implementing passwordless authentication. For instance, voice and facial recognition, retina scan, and biometric verification are all AI-powered features.

Zero Trust Architecture

Zero Trust is a framework that provides comprehensive security for digital infrastructure by validating, authenticating, and authorizing all users before they're granted access to a system. These systems can be local, in the cloud, remote, or a hybrid setup.

Zero Trust works within the following core principles:

- **Continuous Authentication.** The framework continuously verifies access and requests user validation based on different variables, including device, location, user identity, and the type of content requested. These authentication processes are adaptive, so a users' access can be limited dynamically as new files are created or shared.
- **Limited Risk Exposure.** Zero Trust limits the impact of a breach, whether it occurs internally or externally, by limiting the access a malicious actor has.
- **Terminates connection.** Zero Trust can leverage behavioral data from the entire IT stack to terminate suspicious connections to prevent ransomware, malware, DDoS, and other forms of cyberattacks.

The US Federal Government has already called for all federal agencies to modernize their approach to cybersecurity by implementing the Zero Trust framework. Your business should, too.

Microsoft Cybersecurity Resource Center

To follow trends in technology and cyber security architecture, visit the Microsoft Cybersecurity Resource Center. This platform is filled with cyber security resources that your IT team can deploy to enhance performance and protect digital assets. You can read articles, interviews with experts, and whitepapers about emerging cyber threats and security techniques.

Staff Training

Everyone in your organization should understand the importance of cyber security and how to defend against the most common attacks. Hold regular trainings and conduct tests to see how well your team would perform during a real breach attempt. Remember: most successful breaches happen when a well-intentioned employee clicks a harmful link or attachment, or grants access to an impersonator.

Envision Can Help

As cybercriminals become more sophisticated, it is vital for businesses to keep up with emerging solutions to counter threats and upgrade their digital infrastructure. The cyber environment is constantly changing. Investing in a strong defense should be a top priority as your cybersecurity team works to protect your business through 2022 and beyond.

Envision Technology Advisors can help you bring your company up to date with modern cybersecurity solutions. We take pride in offering superior security, business continuity, managed IT, automation, and data analytics services. All our services can be tailored to meet the specific needs of your organization. To learn more, schedule a time to connect with us.

About Envision Technology Advisors

Founded in 1998, Envision Technology advisors provides a wide range of business and technology consulting services to businesses nation-wide. Envision's specialties include Microsoft Consulting & Zero Trust, Cyber Security, Managed IT Services, Data Analytics & Automation, Infrastructure Consulting, Web Design & Custom Development, and Digital Transformation. The company has a commitment to hiring the best talent and building an exceptional work culture, with "Best Places to Work" wins in fourteen consecutive years. For more information, visit www.envisionsuccess.net.