FORTRA

**GUIDE** (Infrastructure Protection)

# Cybersecurity Trends and Predictions for 2022–2023

It's no surprise to cybersecurity professionals that threats have continued to ameliorate and outpace attempts to contain them. War, supply chain issues, continued remote work, and other upheaval create opportunities for cyber disruptors. But organizations may be getting better at preparing for and guarding against intrusion. Governments around the globe have begun to appreciate the possibility of catastrophic consequences if critical infrastructure components aren't protected or private data is leaked. Here is a look at the top cybersecurity trends of 2022 and predictions for coming year from our experts.

# Geo-political and Economic Impacts

## Trends

The Russian war against Ukraine has galvanized supporters far from the battlefield. Cyber warriors for and against both sides have worked to sow disruption using a variety of methods. Ransomware and distributed denial of service (DDoS) attacks continue to cause concern. Zero-day exploits, AI-enabled disinformation, and other attacks, often state-sponsored, have been part of a wider range of threats since Russia invaded Ukraine, according to the European Union Agency for Cybersecurity (ENISA).

While other vectors came into play, there's no denying the significant increase in DDoS attacks. There was a 203% jump in the first half of 2022 compared to the same period of 2021. The scale of the attacks also increased. For example, Google thwarted the largest ever HTTP-based DDoS attack, just a month after Cloudflare stopped a record-breaking one. Another strike that made global news because of its geopolitical implications was carried out against the Taiwanese government. It happened as Speaker of the House Nancy Pelosi was due to visit, something China said it would take action against. In fact, the US Cybersecurity and Infrastructure Security Agency (CISA) listed threats from state actors in Iran, China, North Korea, and Russia during 2022.

Hacking for a cause isn't limited to state-actors though. Consider the moves of abortion-rights hacktivists after the US Supreme Court struck down the guaranteed access granted by Roe v. Wade. A group calling itself SiegedSec hacked the state government servers for Arkansas and Kentucky in protest over those states' bans. The video-game streaming service Twitch and crowdfunding site GiveSendGo were also both targeted by hacktivists on a mission.

## Predictions

Experts predict the uptick in DDoS attacks and hacktivism will continue into 2023. Conflicts between nations and within nations between ideological groups will still result in polarization, leading some to sow chaos and disruption on digital battlefields.

Governments will be compelled to take action, protecting vital cyber architecture. Businesses may face a tougher choice too. As inflation, supply chain issues, and other economic constraints continue to affect organizations around the globe, some will have to make hard budget decisions regarding spending on security measures or on other pressing matters. With increased risks, it could be a roll of the proverbial dice if companies decide to direct their finite funds away from cybersecurity.

DDoS Attacks Up 203% ↑

# New Laws and Regulations

## Trends

In response to ongoing global threats, cybersecurity regulations will continue to evolve. Following the Executive Order on Improving the Nation's Cybersecurity issued on May 12, 2021, Congress passed the Strengthening American Cybersecurity Act (SACA) in 2022. SACA gives federal officials a transparent view of infrastructure cyber attacks nationwide. It helps protect these critical assets by requiring operators of electrical grids, water treatment systems, and other vital interests to notify CISA within 72 hours of a data breach and within 24 hours of any ransomware payments.

The executive order also helped pave the way for cybersecurity measures in the Bipartisan Infrastructure Law (BIL). It includes a grant program with $1 billion in funds for state, local, and territorial governments to shore up their cyber defenses. States are stepping forward with their own measures, as well.

> In 2022, nearly every US state and Puerto Rico put forth cybersecurity bills.

41 were adopted as of mid-year. Common themes included setting up formal training practices, incident response plans, and reporting measures. Others support cybersecurity education, securing elections, and funding all these efforts. In addition, data privacy measures were debated in 25 states and Washington, DC. As of June, five states had enacted six laws governing the collection of personal information, consumer data rights, website privacy, and more.

## Predictions

The executive order is expected to continue to bear fruit in 2023 and beyond as agencies ramp up their cybersecurity efforts. The $1 billion in BIL funding for grants to state, local, and territorial governments will be available across four years. The unprecedented combination of FEMA's grant-administration and CISA's cybersecurity experience is intended to help non-federal agencies understand and mitigate infrastructure risks. Grant applications were being accepted until late in the year so implementation for the first round will come in 2023.

At the federal level, the energy and transportation departments along with the Food and Drug Administration, CISA, and the Federal Trade Commission are all creating new cybersecurity rules. US states are also expected to continue enacting their own data privacy and ransomware payment notice laws.

Overseas, the European Union is fine tuning its General Data Protection Regulation (GDPR) to plug holes created when part of the law was overturned in court. It's also developing ways to allow smooth data transfer out of the EU to other countries, including the US.

Cybersecurity experts will, no doubt, be glad to see all these regulatory efforts come to fruition. Some, however, caution about another approaching issue. As multiple standards are enacted at federal, state, and possibly even local levels, a time could come when regulations collide and contradict each other. There may be a shake-out period where businesses need assistance to navigate the complex regulatory landscape.

# Attack Methods and Prevention

## Trends

As technology continued to evolve in 2022, so did cyber attacks. The year saw additional:

- Supply chain attacks
- Targeted ransomware
- Mobile attacks
- AI-supported cybercrime

Most everyone probably has a personal story of supply-chain issues this year. Part of the problem was the global nature of supply chains and attempts to adjust to pandemic-related changes in work habits and buying habits. But the proliferation of third-party vendors and global networks is a siren call for cyber attackers and they responded. Cybercriminals looking to make a splash, and some cash, will continue to look for opportunities to profit from supply chain disruption.

> Gartner predicts that by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chain.

Ransomware has been a problem for years. After the Colonial Pipeline ransomware case caused panic and fuel shortages along the East Coast, and the nearly $5 million ransom was paid, the White House issued an executive order aimed at shoring up the nation's cybersecurity. Nonetheless, the success of such a high-profile attack just fueled the attraction of ransomware for cyber criminals so more such attacks are expected. Targeting companies and infrastructure assets that have a high likelihood of paying ransoms, like critical infrastructure, will remain attractive for hackers.

With the introduction of 5G and the continued proliferation of IoT devices, attack surfaces have increased. And more mobile devices connected to the faster networks just increases the potential speed of any attacks. Mobile devices are notoriously undersecured, giving experienced cyber criminals the advantage. In fact, platforms for these devices have been responsible for about 70% of financial fraud, usually initiated via phishing and malware.

AI has already delivered good results for business, uncovering process inefficiency and speeding up data analysis. But any technology that can be put to productive use can usually also be employed by attackers and this one is. Deepfake videos and photos are a good example of this. They use artificial intelligence to mimic trusted sources and cybercriminals have been taking advantage.

## Predictions

Next year looks to bring a combination of increased and continued attacks as well as the arrival of some solutions. As more devices join the internet of things and operational technology (OT), malware will break in and spread along networks. As discussed above, AI-created deepfakes make social engineering attacks even easier so expect those to increase as even vigilant people may have a hard time knowing what's real. On the subject of real or fake, a rise in ransom-vaporware is also expected as attackers realize the value in simply threatening to publicize a breach that didn't even happen. Companies may be willing to pay handsomely to keep a jittery public from thinking their data has been exposed. Good old-fashioned ransomware won't be taking a holiday though and will continue to increase.

And then there are electric cars. Electric vehicle (EV) registrations have increased by more than 20% every year since 2018 compared to fossil-fuel powered vehicles' top

growth rate of 1%. An increasing number of traditional vehicles are internet connected, but electric vehicles require sophisticated intra-auto networks (CANbus systems) to keep everything operating together. As sales of EVs rise, expect additional automotive hacks that go beyond taking control of individual vehicles into theft of corporate data using vehicle communication systems to gain entry.

Multi-Factor authentication (MFA) was a boon to security professionals when it first arrived on the scene. Of course, would-be attackers didn't sit still but continued to up their game in response. Inherent flaws in the system will cause strategic adjustments going forward. In 2023, look for cybercriminals to exploit MFA techniques like push notifications. Companies and other organizations will need to move to biometrics, FIDO2, and other passwordless authentication.

As promised, some solutions will also arrive next year. Following the White House push for increased cybersecurity, including requiring government software to be zero-trust, expect products to actually be zero-trust ready. It should also be easier to find products that satisfy all seven tenets of the National Institute of Standards and Technology (NIST) 800-207 model, and support architecture referenced in NIST 1800-35b.

# Organizational Behavior

## Trends

Cyber insurance is increasingly considered a business requirement, especially for tech companies or organizations that handle sensitive information. But it's also becoming increasingly expensive. In the second quarter of 2022, US cyber insurance prices were already 79% higher than the previous year. And the increase in attacks means insurers have to cover their own risks by setting coverage limits and requiring strict cybersecurity measures before they issue a policy. Some insurance carriers have also reduced the coverage they are willing to offer high-risk industries such as critical infrastructure. Regardless, businesses understand the need for cyber insurance and have continued to purchase it. As more companies demand it and insurers restrict it or charge higher rates, fewer organizations may actually be able to find or afford it.

Just as insurers are frequently demanding strict cybersecurity measures as a condition for coverage, organizations are making similar demands. It's becoming more common for potential partners, acquirers, and others considering third-party business agreements to scrutinize security postures and protocols as part of the vetting process. Companies and others are starting to pay much more attention to the security of their entire digital supply chain.

As organizations became more aware of the need for information security, they appointed chief information security officers (CISOs). Now the trend is swinging back the other direction with the CISO acting more as a risk manager of a decentralized cybersecurity apparatus with decision makers throughout the organization. This gives companies the ability to respond quicker and with greater agility than having all the response power in one person or office.

One other trend is the introduction of cybersecurity mesh architecture (CSMA), a term coined by tech consulting firm Gartner. Today's workers and business assets may or may not be located in a company office or other central space. CSMA is part of a larger security network that can work hand in hand with zero trust and other measures to secure enterprise assets wherever they are located, in the physical world or the cloud. Companies that use CSMA will reduce the impact of discrete security incidents by 90%, according to Gartner.

## Predictions

As part of the move to decentralize cybersecurity oversight, expect to see boards of directors, CEOs, and other leaders participating in cyber risk decision making and governance. It is also likely that those corporate leaders will embrace the comprehensive, integrated approach to cybersecurity provided by CSMA.

The trend of more stringent third-party vetting processes will continue along with increased third-party liability for security incidents. Vendors, suppliers, partners, and others in the data supply chain could find themselves facing lawsuits if their lax security facilitates access for cyber criminals.

**Finally, expect to see vendor and tool consolidation as organizations seek to gain efficiency and reduce complexity of security functions**. In fact, it's expected that by 2025, 80% of enterprises will adopt integrated security service edge (SSE) solutions that will enable them to effectively unify access to the web, cloud, and private applications from a single platform.

# A Brighter Future

Gone are the days of being caught off guard by cyber attacks. Organizations large and small are aware of the risks and increasingly taking steps to mitigate them. From zero trust to cyber insurance to CSMA, tools are being deployed to plug the holes that allow cyber criminals to gain entry. Even the US government has gotten on board and, in some cases, pushed others to take appropriate measures. Of course, the bad actors won't sit still so ever more vigilance will be required going forward. Cybersecurity must continue to evolve in hopes of staying ahead.

At Fortra, we're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions – including vulnerability management, penetration testing, red teaming, data protection, secure file transfer, and digital risk protection, email security and anti-phishing and security services - bring balance and control to organizations around the world.

FORTRA

Fortra.com

**About Fortra**

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.