Experian® 2022 Data Breach Industry Forecast

NINTH ANNUAL EDITION

Executive Summary

The year 2021 began with cautious but genuine optimism in much of the world, buoyed by the twin effects of a new U.S. administration, and the hope that, with new vaccines, the COVID-19 pandemic would soon end. That optimism faded somewhat as the year unfolded, as new strains of COVID-19 emerged, natural disasters reminded us of ongoing climate change, and new cyber threats emerged from our ever-more digitally intertwined world. People across the globe have never been more digitally connected than now. While that connectivity enables amazing new technological capabilities, it also constantly creates new vulnerabilities.

In a sense, 2022 will be a sort of hangover from 2021's "cyberdemic." Since so much of our lives now take place online, the digitization of society means that our infrastructure, institutions and personal lives are more exposed than ever to malicious actors. Big institutions remain vulnerable, despite spending millions on security, and cybercriminals have plenty of opportunities to exploit weak technologies.

Our world is not going to become less interconnected any time soon – and many more data vulnerabilities and cyberattacks will be uncovered in the upcoming year. In the Ninth Annual Experian Data Breach Industry Forecast, we look at five areas we believe are most likely to be targeted for cyberattacks in 2022.

Our predictions come from Experian's long history of helping companies navigate breaches over the past 18 years.

Based on Experian's expertise, the top data breach trends in 2022 include the following:

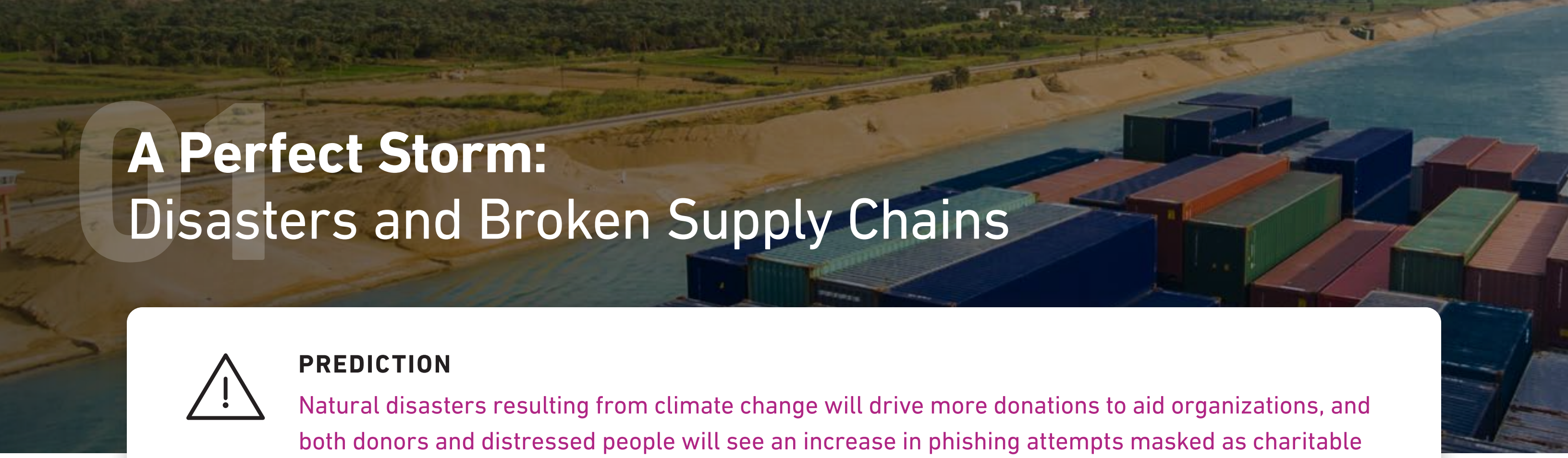
- **Perfect Storm: Natural Disasters and Broken Supply Chains**
  Natural disasters will drive more donations to aid organizations, and both donors and people in distress will see an increase in phishing attempts masked as charitable giving. This will be complicated by broken and unreliable global supply chains that will make the sourcing of important emergency goods difficult – another vulnerability that hackers will look to exploit.

- **Hackers Bet on New Gamblers**
  As more states legalize online sports betting, phishing scams will target the growing ranks of online gamblers, particularly new entrants. The large pool of money flowing from gamblers to online casinos will be a tempting target. The fact that gambling is increasingly legal will make online fraudsters harder to detect. Relatedly, scammers will also target fantasy sports sites, whether through phishing attempts or outright hacks.

- **Cyberdemic 2.0: Institutions Adapt, Individuals Remain the Weak Link**
  It's clear now that many of the adaptations we made suddenly in response to the pandemic – telehealth, remote work, contact tracing – have left imprints on society that will outlast the pandemic itself. Some of these changes are now permanent aspects of our lives, arguably with mixed consequences. While many institutions will have successfully adapted by 2022 and developed new security protocols, many individuals – still working remotely – will likely be the weak security link in these new digital systems.

- **Digital Assets Put Us in Peril**
  Cryptocurrency arguably entered the mainstream last year, and NFTs (or Non-Fungible Tokens) are not far behind. As people increasingly accept these as legitimate transactions and legitimate asset classes, both will become targets for attack, revealing that these ostensibly safe, immutable assets are in fact vulnerable. Concurrently, as our identities become more digitized, more bad actors will look to leverage these assets as a way to steal identity.

- **Infrastructure: New Roads to Theft and Destruction**
  Cyberattacks have generally sought either disruption or extortion, but soon both state and non-state actors will more frequently target physical infrastructure like electrical grids, dams, or transportation networks. Relatedly, hackers will target funds disbursed by Congress that are intended to rebuild U.S. infrastructure.



01

A Perfect Storm: Disasters and Broken Supply Chains

PREDICTION

Natural disasters resulting from climate change will drive more donations to aid organizations, and both donors and distressed people will see an increase in phishing attempts masked as charitable giving requests to support communities in need. This will be further complicated by unreliable global supply chains that will make the sourcing of important emergency goods difficult – another vulnerability that online thieves will look to exploit.

From Hurricane Ida, to global wildfires, to the catastrophic floods in China and Western Europe, 2021 had more than its share of devastating natural disasters, and some climate scientists predict that the years to come will be even worse.

Catastrophes tend to drive charitable donations to people and communities hit by them. In 2018 roughly 30% of American households made a disaster-related charitable donation. With this much money changing hands, expect cyber criminals to see an opportunity, much like contact tracing apps for COVID were in 2021.

The problem is already widespread enough that last year the Federal Emergency Management Agency put up a website warning people to "be wary of hurricane-related scams and rumors about financial relief," as the agency received more than half-a-million imposter fraud claims in the first half of 2021.

Some of these scams are familiar: online donation requests from reputable-looking organizations ostensibly for communities hit by disasters, or requests for aid directly from people purportedly victimized by disaster, either directly or through fundraising websites. Sometimes other methods are used, like when cyberthieves stole nearly $1 million from a Philadelphia food bank by creating fake invoices.

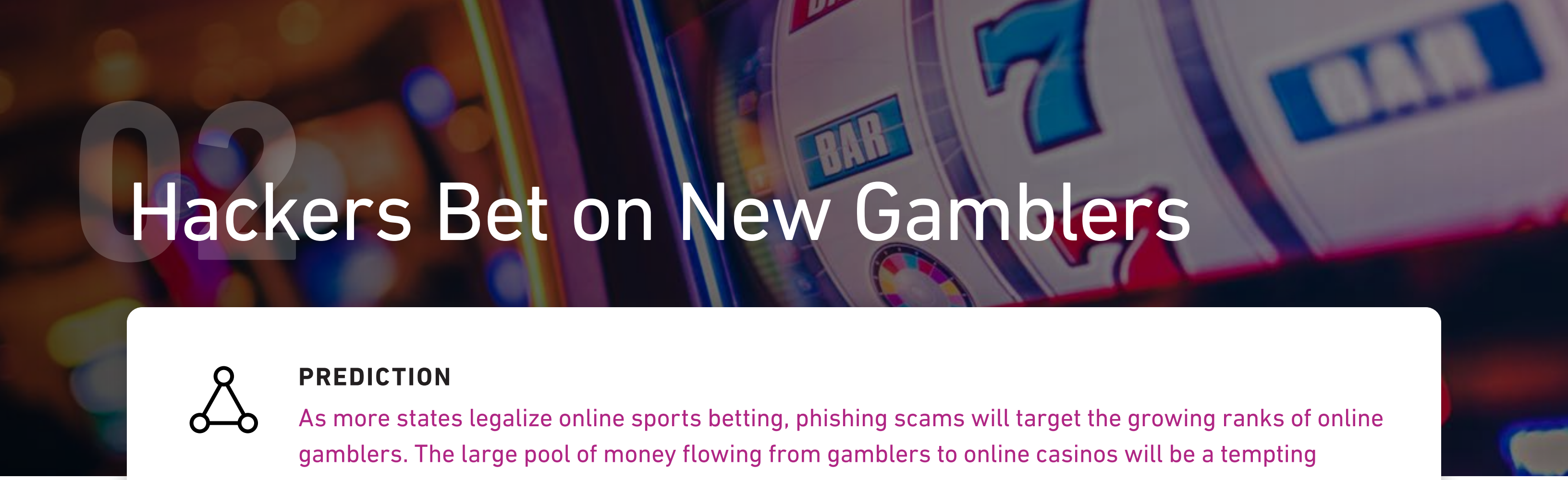
What will be different next year is that natural disasters will coincide with ongoing and sometimes crippling supply chain problems across the U.S., a problem that some forecasters don't expect to end for some time.

In response, thieves will impersonate legitimate vendors selling scarce items in high demand – be they masks, personal protective equipment, oxygen or other critical items.

One trouble with preventing this sort of fraud is in the nature of how people respond to disasters: with lives at stake, urgent decisions by relevant authorities have to be made quickly, sometimes foregoing customary due diligence. A hypothetical: Imagine a hurricane taking out power or overwhelming sewers in a Gulf Coast city – would local FEMA workers have time to check the veracity of every single supplier or contractor, confirming that they are who they say they are, before deciding to purchase badly needed supplies?

THE TAKEAWAY:

The wreckage of natural disasters and fragile supply chains will create tempting targets for cyber thieves looking to exploit tragedy. First-responders often have to make quick decisions, and people making donations to charities in response to disasters are often motivated by the kind of empathy that doesn't always ask questions. Both conditions are ripe for online scammers presenting as legitimate vendors or philanthropic organizations. If you're in the former category, take the time to make sure that every vendor claiming to provide life-saving or mission-critical materials is who they say they are. If the latter, check with an organization like CharityWatch to determine that the organization you want to give to is the real thing. Don't take that online vendor or charity's profile at face value.



02

Hackers Bet on New Gamblers

PREDICTION

As more states legalize online sports betting, phishing scams will target the growing ranks of online gamblers. The large pool of money flowing from gamblers to online casinos will be a tempting target. The fact that online gambling is increasingly legal will make fraudsters harder to detect. Relatedly, scammers will also target fantasy sports sites, whether through phishing attempts or outright hacks.

Online gambling is already a huge business, estimated to be $72.02 billion globally in 2021. But its growth has been held back somewhat in the U.S. by conflicting state laws. While at least 10 U.S. states have legalized some form of the activity – whether sports betting, poker or casino gambling – many more are considering easing restrictions or outright legalizing, tempted by the prospect of tax windfalls. In the summer of 2021, the nation's four most-populated states – California, Texas, Florida and New York – all made steps toward making the practice legal.

Even in states where casino gambling isn't legal, online gambling is growing fast. As of 2017, 61% of casino revenues came from online bets, with 72% of those bets cast from mobile devices.

The pandemic has brought forth a whole new market for this enterprise, as more people than ever were stuck at home with their computers and mobile devices.

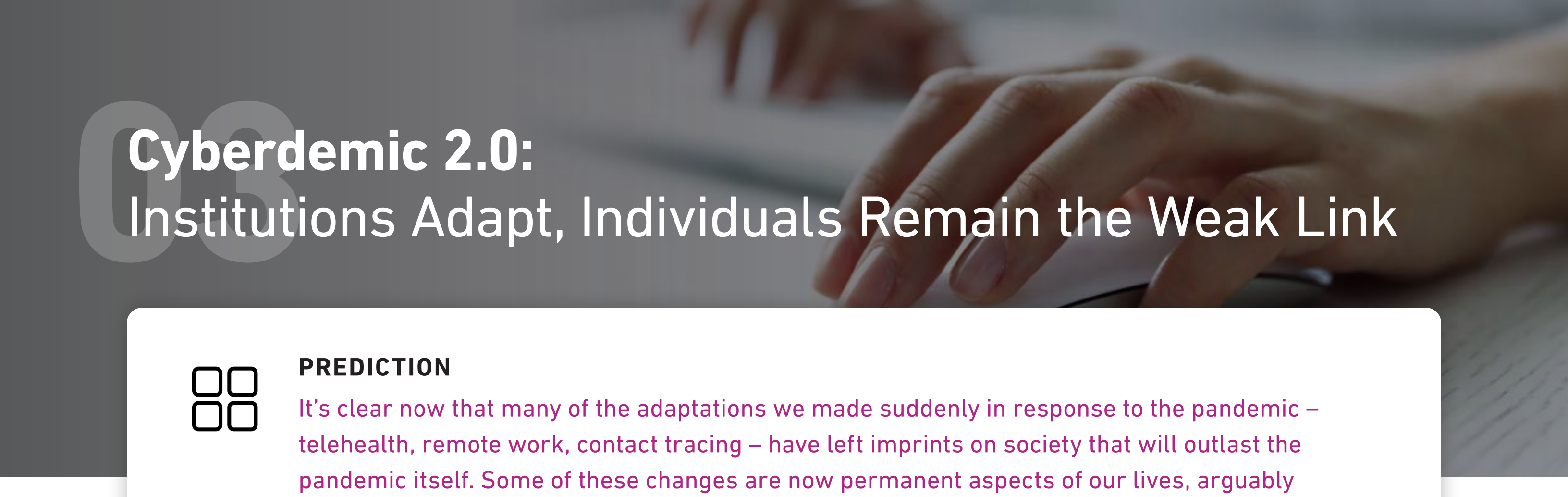
It's a large and growing business, with lots of available cash, and has thus attracted the interest of online thieves. Common forms of thievery here include gambling using stolen credit card info, taking over an account through hacking or correctly guessing a password, or impersonating a legitimate online casino.

Hackers will also be more brazen in targeting the platforms themselves, not just the gamblers. For an example of how that could look, refer to the 2020 hack of DraftKings, where the online gambling and betting site was hit with a DDoS and ransomware attack. And while cyberattacks on fantasy sports sites aren't unheard of, expect them to become much more common as more people get involved with this activity.

Cryptocurrency is also increasingly popular in online gambling – and more sites are facilitating its use. Expect hackers to use this as a means to break into digital wallets, especially during times when bitcoin is soaring in value.

THE TAKEAWAY:

Online gambling – whether sports, poker, or casino – is more popular than ever, but it carries many opportunities to have your money stolen. Learn about what some common scams look like and make sure to look out for identifying signs. Legitimate online casinos generally display their licenses clearly and have reliable and transparent customer service. The lack of a padlock on the URL, or the lack of Google search results for an alleged casino site are red flags.



03

Cyberdemic 2.0:
Institutions Adapt, Individuals Remain the Weak Link

PREDICTION

It's clear now that many of the adaptations we made suddenly in response to the pandemic – telehealth, remote work, contact tracing – have left imprints on society that will outlast the pandemic itself. Some of these changes are now permanent aspects of our lives, arguably with mixed consequences. While many institutions will have successfully adapted by 2022 and developed new security protocols, many individuals – still working remotely – will likely be the weak security link in these new digital systems.

In 2021 the national conversation centered around a 'return to normal' post-COVID-19, but as 2022 dawns it's clear the pandemic advanced some trends that are not likely to reverse. The quick adaptation to new forms of work and recreation – remote work, Zoom calls, telehealth screenings, to name a few – in many cases required either the scaling up of existing IT infrastructure, or the installation of entirely new systems.

At first these new patterns of living created a lot of chaos that cyberthieves were able to exploit – think of the large number of successful ransomware attacks on homes, hospitals, and other businesses last year. Responses to the pandemic like contact tracing apps and QR codes in retail establishments all became vectors of potential fraud. And as people hunkered down at home, their smart devices became new vulnerabilities.

But in 2022 – in what we're calling Cyberdemic 2.0 – the vectors will have shifted a bit. Enterprises that suddenly went fully remote now have a better handle on at least some of the necessary security IT protocols. Hospitals experimenting with telehealth services in 2020 and 2021 have increasingly made it a part of their business offering. Businesses and municipal governments have largely adapted to contact tracing and digital proof of vaccination. (Interestingly, though, the threat to companies is still seen as severe enough than many insurance companies are no longer offering insurance against hacks.)

This means the vulnerabilities cybercriminals will look to exploit will largely be individuals, particularly those who are still working, learning, and playing remotely.

Despite many workplaces reopening, there will still be a lot of people working remotely. According to a LinkedIn survey of nearly 3,000 American workers in July 2021, [36% of employees working remotely were still waiting for their employer to decide]() if workers will return to an office or stay remote.

Since home wireless networks are still more vulnerable than many business VPNs, enterprises will need to focus more on security compliance from employees. Employees will need training on matters like how to spot a phishing attempt, or how to respond to a ransomware attack.

Even though enterprise IT – whether on premises or on the cloud – is on the whole safer than a two years ago, cyberthieves will of course still be targeting companies' networks. But the remote worker will likely turn out to be the more tempting avenue into the company's information coffers.

THE TAKEAWAY:

Even as the pandemic itself recedes into being something resembling an endemic – meaning a fact of life that we must mitigate risk against rather than exist in a perpetual state of emergency – certain of our newly adopted habits are here to stay. And while many enterprises will have adapted will to the new environment by 2022, a significant amount of sensitive data remains on company premises, and will be a tempting ransomware target as IT workers struggle with complex security protocols in a remote-first work environment.

04 Digital Assets Put Us in Peril

PREDICTION

Cryptocurrency has been in the cultural lexicon for many years, but arguably everyday use grew in popularity last year. NFTs (Non-Fungible Tokens) are likely not far behind. As people increasingly accept these assets as legitimate transactions – or at least as legitimate asset classes – both will become vulnerable targets for attack, revealing that these ostensibly safe, immutable assets are in fact vulnerable. Concurrently, as our identities become more digitized, more bad actors will look to leverage these assets as a means of identity theft.

One of the most hyped stories of 2021 was the rise of the NFT, or "non-fungible token," a unique, imutable digital asset that was hailed by some as a savior of the music industry, and pilloried by others as a worthless status symbol for the rich.

It's also another indicator that identity and value have become more ephemeral as they move online. Like blockchain – similarly hyped a few years back, though now it's being productively used in certain applications – NFTs remind us that innovations are far from exhausted in the digital age.

And where value – or perceived value – goes, thieves and bad actors will follow. While the concept of the NFT was still novel in the public mind in 2021, one unfortunate buyer paid $300,000 in Ethereum for a NFT of a Banksy artwork that turned out to be counterfeit. The scammer ultimately returned the money, but the proof of concept was demonstrated.

Blockchain is touted by nearly all of its proselytizers to be unchangeable once a transaction is lodged, but there are apparently plausible ways of overcoming this. So-called 51% attacks are a way hackers could disrupt or alter a chain.

But the adoption of these digital assets – and relatedly, using digital assets as identity markers – shows no sign of slowing down.

Big tech companies are making it easier to push more of our traditional markers of identity into the digital realm. Apple, for one, is looking to partner with states to digitize personal identification – including, but not limited to, driver's licenses – and this will make your smartphone vulnerable in yet another way. The attention garnered by Pegasus spyware this past year, which can take over a smartphone with a single text message, reminds us how vulnerable our phones are to being hacked and taken over, even when the smartphone maker prioritizes security in its products.

THE TAKEAWAY:

As cryptocurrencies and NFTs become more commonplace and are increasingly accepted as legitimate parts of our financial and technological landscape, both will become targets for attack. The combination of a cryptocurrency transaction with distributed ledger technology make NFTs uniquely positioned for multiple points of vulnerability.

05

Infrastructure: New Roads to Theft and Destruction

PREDICTION

Most cyberattacks to-date have sought either disruption or extortion, but soon both state and non-state actors will become more brazen, targeting physical infrastructure like electrical grids, dams, or transportation networks. Congress' effort to rebuild outdated U.S. infrastructure will mean enormous budgetary outlays that will be an ideal target for hackers, particularly foreign actors who see a dual opportunity in both financial gain and disruption of U.S. development efforts.

U.S. infrastructure was perhaps the single most significant piece of legislation introduced in Congress in 2021, and hackers will take a keen interest in it next year as the funds to rebuild are set to be disbursed and new vulnerabilities in networks that underpin our society are discovered.

American roads, bridges and energy grids have all needed substantial upgrades for many years, and it appears that in 2022 Washington will finally fund these endeavors. This effort will create millions of jobs, keep the U.S. competitive globally and help mitigate climate change, meaning huge budgetary outlays of multiple trillions of dollars for years to come.

Hackers will target this primarily in two ways.

First, foreign or domestic actors will aim to steal some of the trillions of dollars allotted by Congress during the process of their disbursement, through phishing, CEO fraud, or other scams. The sums are so large, and their distribution involves so many institutions and processes – from the Treasury to vendors, to banks, to individual contractors – that hackers will be probing for weaknesses in the money supply chain.

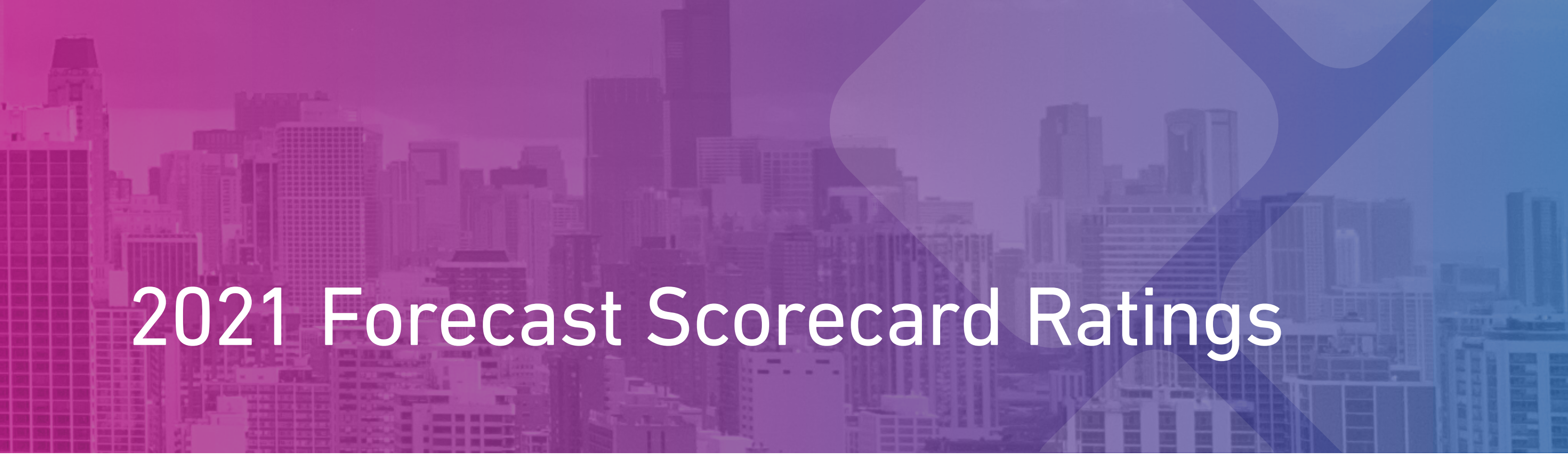
Second, hackers – largely foreign – with enmity toward the United States will be more brazen in their efforts to disrupt domestic infrastructure like electrical grids, energy pipelines or manufacturing facilities.

Some of this has already been foreshadowed. The Colonial Pipeline hack in the Spring of 2021, which shutdown the major conduit for oil all along the U.S. Eastern Seaboard, was done for money, rather than geopolitical reasons. The company ultimately paid a ransom to a criminal gang called DarkSide to restore gas flow. There's no guarantee that other, similar attacks won't happen out of sheer malice. JBS Food and Kia Motors were among the many other companies targeted for ransomware attacks in 2021, as were a Florida city's water supply and a San Diego hospital system.

Adding to this temptation will be perceived U.S. weakness – whether valid or not – after decades of unchallenged supremacy on the global stage. The apparently chaotic withdrawal from Afghanistan, and the perceived irresolution of Washington will likely embolden U.S.'s global adversaries – China, Russia, North Korea, Iran – to target infrastructure here.

THE TAKEAWAY:

Cybersecurity experts involved in critical infrastructure or disbursement of funds should be extra alert to being targeted by domestic or foreign hackers. If you're a vendor involved with U.S. infrastructure projects, double check to make sure vendors can be verified. When managing critical infrastructure, make sure that your security and software providers are up to date and can accurately assess the constantly shifting threat landscape.



2021 Forecast Scorecard Ratings

A+

Vaccine Ripple Effect

As the world races toward a COVID-19 vaccine, cybercriminals may try to capitalize on global anxiety by spreading misinformation and conspiracy theories. This has the potential to create global uncertainty and panic. These same criminals could also plot to disrupt vaccine supply chains and impact vaccine availability for countries, creating a new kind of pandemic warfare.

UPDATE

Cybercriminals rarely miss an opportunity to exploit new system vulnerabilities, and the organized responses to the COVID-19 were no exception. The spread of misinformation through social media contributed to widespread doubt about the efficacy of the vaccine, and nation-state hackers targeted various companies involved in the global vaccine supply chain. Billions of people across the world nevertheless have received one of the various vaccines, so authorities were able to make progress nonetheless, but the fact there remains a substantial amount of vaccine hesitancy, particularly in the U.S., shows the power of deliberate misinformation.

B-

Home Devices Held for Ransom

With families spending more time in their homes than they have in decades, cybercriminals will target individuals by using connected devices to carry out attacks. These attacks can be particularly malicious, going as far as holding wealthy families or celebrities hostage in their homes for ransom. We predict in 2021 that at least one wealthy family or celebrity will experience a takeover situation via their connected home devices.

UPDATE

Even though their public profile and resources make them an ideal target, no major cyber-attacks were made against stars or wealthy individuals in 2021. Perhaps closest was directed against the NBA's Houston's Rockets, which suffered a ransomware attack by the hacker group Babuk, resulting in the theft of 500GB of confidential data. Another, somewhat related version: Chinese hacker group APT31 used home routers in France in order to disguise their origin. It reminds us that as connected technology becomes more deeply embedded into the fabric of our homes, these attacks will be more common in the future.

B

Without a Trace

As COVID-19 spread, there were tracking systems put in place for new infections to keep vulnerable populations safe. Contact tracing applications will probably continue to be developed to track the spread of COVID-19 around the world. Cybercriminals may seek to exploit these types of application programming interfaces (APIs) to gain access to personal user information and wreak havoc in 2021.

UPDATE

As with any digital product developed quickly, COVID-19 contact tracing apps have their vulnerabilities, and hackers did not hesitate to exploit them. One of the more significant exposed the information of 72,000 individuals in Pennsylvania. State officials blamed the vendor not following correct protocol. While not as serious or as widespread as other kinds of cyberattacks, and likely somewhat easier to fix, these apps will remain a potential threat vector as long as they are used to monitor the spread of disease.

B-

5G Has a Weak Spot

5G is making its way to your connected devices soon, if it's not already there. It's a next-generation wireless technology that's expected to make waves, from cell phones to self-driving vehicles. What makes 5G unique is its speed. What makes it concerning is the billions of new endpoints susceptible to attack.

UPDATE

This prediction was a little premature, as 5G has not quite become the ubiquitous network many imagined it would be by now. This doesn't mean the threat is nonexistent, of course, and it's safe to say that 5G networks are an emerging threat vector. So much so, that federal agencies like the Department of Defense made the securing of emerging 5G networks a major priority in 2021. Expect this to become a greater concern in the years to come.

A

Digital Health: A Blessing and a Curse

Yesterday's patient is accustomed to overwhelming healthcare paperwork and thinks of telehealth as a lesser alternative to in-person doctor visits. But in 2020, the trend of digital services and telehealth took off due to social distancing and COVID-19 remote screenings. Offices without online scheduling or a telehealth plan had to play catch-up in a matter of weeks. We predict this hurried effort will present an opportunity for major cyberattacks in healthcare, exposing thousands of patients' personal and medical records.

UPDATE

As previously mentioned, health care facilities were a top target of hackers in 2021. Millions of people fell victim to telehealth attacks that stole personal records, or subjected institutions to ransomware, which many had no choice but to pay. Some of the biggest were the Florida Healthy Kids Corporation (3,500,000 health care records exposed), NEC Networks (1.6 million records) and American Anesthesiology (1.2 million records). The rapid transition to remote medicine that many medical facilities underwent did not always include rigorous cyber safety protocols. Hospitals will continue to be a target for cyber criminals until they retrofit these new systems with better security.

About Experian Data Breach Solutions

Experian® Data Breach Resolution

Experian Data Breach Resolution, powered by the nation's largest credit bureau, is a leader in helping businesses prepare for a data breach via the proprietary Experian® Reserved Response™ program and also mitigate consumer risk following breach incidents. With more than nineteen years of experience, Experian has successfully serviced some of the largest and highest-profile data breaches in history. The group offers swift and effective incident management, notification, call center support and fraud resolution services while serving millions of affected consumers with proven credit and identity protection products.

Reference Links

https://www.experian.com/blogs/news/2021/02/03/2020-cyber-demic-whats-come/

https://www.nationalgeographic.com/environment/article/deadly-heat-waves-floods-drought-will-get-worse-if-warming-continues

https://disasterphilanthropy.org/wp-content/uploads/2019/06/US-Household-Disaster-Giving-one-pager.pdf

https://www.forbes.com/advisor/personal-finance/hurricane-ida-scams/

https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/CategoriesRanked

https://www.nbcphiladelphia.com/news/local/broke-in-philly/cyber-thieves-targeted-philabundance-in-a-scam-this-year/2616800/

https://www.forbes.com/sites/garthfriesen/2021/09/03/no-end-in-sight-for-the-covid-led-global-supply-chain-disruption/?sh=21056fba3491

https://www.charitywatch.org/top-rated-charities

https://www.thebusinessresearchcompany.com/report/online-gambling-global-market-report

https://gamblersdailydigest.com/online-casino-sports-betting/

https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/draftkings-targeted/

https://www.coinspeaker.com/crypto-used-online-gambling-industry/

https://www.legitgamblingsites.com/blog/five-tips-to-avoid-online-casino-scams/

https://www.cnbc.com/2021/08/16/linkedin-36percent-remote-workers-await-employer-return-to-office-plan.html

https://www.forbes.com/sites/michaeldelcastillo/2021/08/13/are-nfts-the-new-napster-this-time-the-music-industry-isnt-taking-chances/?sh=6d47d29c5a90

https://micky.com.au/nfts-emerging-as-the-new-status-symbol/

https://www.theverge.com/2021/8/31/22650594/banksy-nft-scam-pranksy-ethereum-returned-duplicates-art

https://www.investopedia.com/terms/1/51-attack.asp

https://www.npr.org/2021/09/02/1033675691/drivers-license-apple-iphone-apple-watch-tsa

https://illinois.touro.edu/news/the-10-biggest-ransomware-attacks-of-2021.php

https://www.ft.com/content/3a6941ce-8b0f-40b1-84d6-6418d8a84c94

https://apnews.com/article/coronavirus-data-privacy-technology-business-health-4b9a172a90bc1a82f83e6a44ff06a445

https://threatpost.com/mobile-operators-5g-security-vulnerabilities/167354/

https://governmentciomedia.com/security-piece-5g-implementation-puzzle