10TH ANNUAL EDITION

Experian® 2023 Data Breach Industry Forecast

experian

Executive Summary

A record year for data breaches in 2022 is unlikely with the figure at 1,291 in Q3, according to the Identity Theft Resource Center. However, that doesn't mean organizations can become complacent. Last year was a record-high with 1,862 breaches reported. Potent, high-profile breaches targeting healthcare, finance, government, and energy entities in recent years prove no company is too large or industry immune, and the ramifications of this ever-expanding onslaught of threats are far-reaching.

In 2022, we saw two of the most significant breaches occur in the cryptocurrency space, recalling one of this report's 2020 trend forecasts that stated cryptocurrency exchanges were likely to become lucrative targets for hackers. Major data breaches also impacted many consumer brands like Uber, American Airlines, North Face and Door Dash.

2022 also solidified that remote work is here to stay. As companies hastily adopted systems and processes to enable employees to work from home amid the chaos of early 2020, many did so thinking they'd only need them temporarily. Now that the hybrid model is a mainstay in the workplace, organizations must cement cybersecurity measures to mitigate the increased risk that comes with employee devices and home networks now serving as primary connection points for some employees to company systems and sensitive information. To solve this challenge, companies would be wise to implement more intensive protocols and security measures, including new cybersecurity software, VPNs and firewalls; enhanced employee training; complex password requirements; regular internal phishing tests; and more to protect their organizations.

The increased use of cyber operations as a tool for exerting influence or seizing power, including by governments and militaries around the world, could raise the prospect of more disruptive cyber activity in the year ahead. Amid surging political tensions and international conflict, defense systems, data centers and digital infrastructure are all potential targets. We've already seen this at play in 2022 when communications in Ukraine were disabled by hackers ahead of Russia's February invasion of the country. In a rapidly changing world where bad actors are more adept at infiltrating sectors vital to daily life than ever, securing critical infrastructure continues to prove essential for countries and organizations worldwide.

In our tenth annual edition of this Data Breach Industry Forecast, we explore the ever-growing frontier for cybercriminals as modern technology like the metaverse opens fresh real estate to attack. We also observe conditions that necessitate a market shift away from insufficient approaches largely focused on prevention and the move toward a focus on cyber resilience and recovery in the face of these attacks.

Cyber resilience is the ability to recover operationally and reputationally from a cyberattack that was not fully mitigated. Organizations will never be 100% protected from cybersecurity threats, but quick detection and defense in the wake of discovery can alleviate potential harm to organizations and consumers. This should be the strategic mindset for companies come 2023 and beyond.

Meet the expert
Michael Bruemmer
Vice President, Global Data Breach and Consumer Protection,
Experian

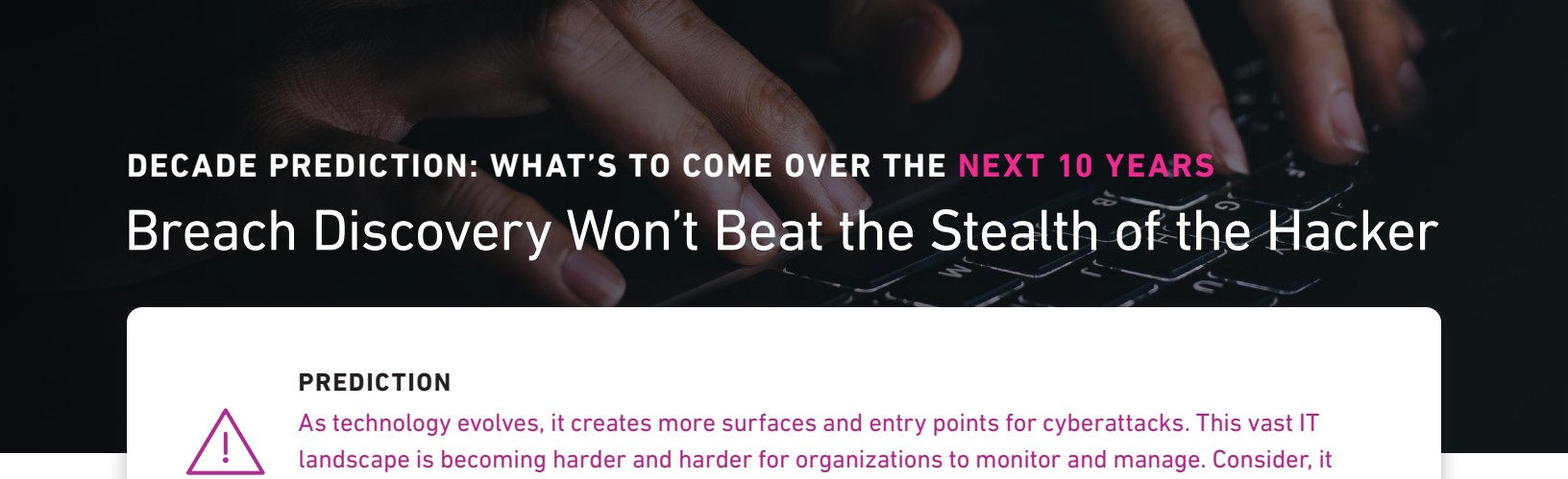
*Contributions also by Brian Stack, Vice President of Dark Web Intelligence, Experian

Executive Summary

Our predictions come from Experian's long history of helping companies navigate breaches over the past 19 years. To commemorate our 10th annual edition, we have an outlook for the next decade and five predictions for 2023, which are the following[1]:

- **Decade:** Like trying to find a pebble in the ocean, detecting an intrusion within what is an ever-growing landscape to monitor keeps cybersecurity professionals up at night. As the vast breach surface continues to increase and the number of devices individuals use to work, play, and transact with multiply, so too does vulnerabilities bad actors can exploit. It's no surprise, it still takes companies more than 200 days on average to detect an intrusion. Thus, the amount of time to detect and defend against a cyberattack will continue to be a sore point and not improve much over the next 10 years.
- Curiosity about the metaverse is increasing. As more people venture into this burgeoning universe, hackers will exploit their inexperience and the vulnerabilities of this cyber frontier. Individuals and businesses should proceed with caution and remember that the safety rules of the 2D online world apply in the digital/virtual realm as well.
- Our growing reliance on satellite-dependent technologies, the increase in the number of satellites in space, and a lack of regulatory oversight mean the likelihood of satellites being hacked is material and the effects of this could be broad. Organizations with space-based assets, or even NASA, that do not shore up protections and remain vigilant will find themselves under attack.
- AI is amazing innovation that can reap many positive rewards. It's a powerful ally to companies including for their cybersecurity defenses, but it's also a potent tool for hackers looking to carry out more attacks, including deceptions that present as highly credible. Organizations must remain vigilant and a step ahead of bad actors capable of weaponizing AI.
- Identity theft has evolved beyond stolen social security numbers and passwords. Deepfake technology lets cybercriminals steal people's actual images and likenesses and impersonate them to serve their own interests. These types of attacks are increasing and may not be exploited just for fun memes in the future. Rather, we may see more strategic attacks from countries in conflict and global hackers who will use high-profile individuals like world leaders to spread misinformation and cause chaos. So don't always believe what you see.
- We've witnessed our first strategic use of cyberwarfare complementing boots on the ground this year, and we foresee that cyberwarfare will be a major part of conflicts in the future. It may even become the first strikes a nation conducts to cripple the opposition before even stepping foot on soil. Could that lead to fewer combat soldiers and more cyber specialists in the military? Not so fast, but if you're interested in cyberspace, Uncle Sam wants you.

[1]The Data Breach Industry Forecast is Experian's attempt at looking into our crystal ball and providing cybersecurity predictions for what may lie ahead. The predictions are not guaranteed, should not be relied on as formal advice and are intended for educational purposes only.



DECADE PREDICTION: WHAT'S TO COME OVER THE NEXT 10 YEARS

Breach Discovery Won't Beat the Stealth of the Hacker

PREDICTION

As technology evolves, it creates more surfaces and entry points for cyberattacks. This vast IT landscape is becoming harder and harder for organizations to monitor and manage. Consider, it takes organizations more than 200 days on average to detect a data breach. This hasn't improved much in many years, and we don't expect it to over the next decade. It's too difficult a game of cat and mouse.

The rise of deepfakes, the rapidly advancing sophistication of AI, our collective shift to the metaverse, and government actors waging cyberwarfare are only the beginning. As societal shifts continue, cybercriminals will become more emboldened in their actions as they uncover new ways to exploit organizations and everyday citizens.

Cyberattacks have evolved at an unprecedented rate over the past decade, costing organizations $2.9 million every minute. Yet, organizations remain slow to identify and contain attacks. An IBM report reveals that on average, it takes 212 days for organizations to identify a cyber intrusion and 75 days to contain it. In many instances, third-party vendors spot the breach before the organization does. Leading cybersecurity company FireEye explains in its 2021 M-Trends report that while companies are getting better at detecting breaches, only 59% identify the hack internally. The rest are noticed by someone outside the company. This is an issue that will continue to persist for at least the next decade.

Why? The threat landscape is simply too vast and growing more rapidly than resources and manpower can manage. As organizations move to and within the cloud and increase the number of access points to their network due to remote work, they provide more openings for hackers to exploit. Cisco has predicted there will be three times more networked devices on Earth than humans by 2023 – translating to nearly 10 devices and connections per household.

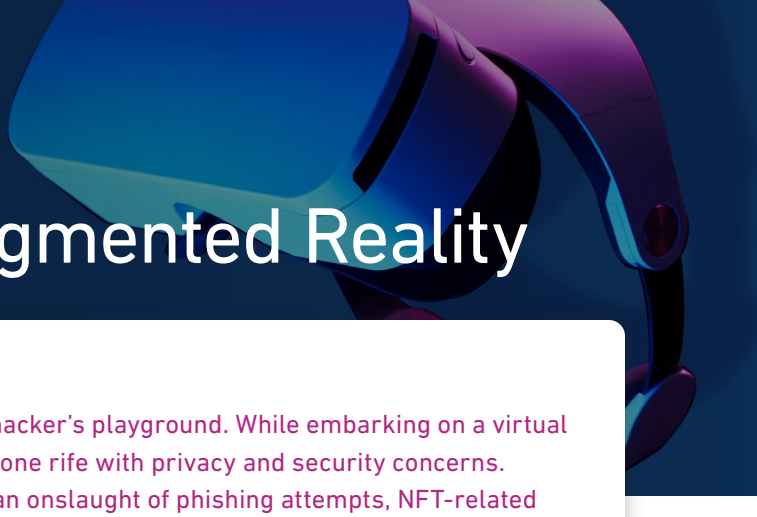
What's more, cyberattacks typically are not large, singular-breach events that are easy to detect, but rather an ongoing process with multiple steps. Cybersecurity and application delivery solutions provider Radware explains that once hackers gain access to an organization's network, they identify what type of access they have and where sensitive data is stored. Then, they play the long game to avoid raising suspicion. Slowly, in a series of small moves not egregious enough to throw up high-security red flags, they infiltrate the network, steadily gaining more access to desired data.

The longer intrusions remain undetected, the more costly and damaging they become. Costs include lost revenue, data and intellectual property. There can also be impacts on an organization's reputation and its relationship with customers and partners. According to data analytics and security firm Varonis, organizations can even incur fines and face legal action from consumers and independent agencies if they take too long to disclose a breach.

Quick detection of cyber breaches is critical. Varonis reports "companies that contain a breach in less than 30 days save more than $1 million in comparison to those who take longer."

THE TAKEAWAY:

The threat landscape will continue to evolve and increase alongside innovation. We don't foresee much improvement in the amount of time it takes to detect and contain an intrusion, unfortunately. One reason is simply because of the increasingly vast landscape that companies need to monitor and manage. While cyberattacks are not going away and it's impossible to create an impenetrable network, organizations should look to stay attuned to precursors such as public advisories or alerts from security experts and shore up vigilance for indicators that there may be an intrusion. The sooner you can detect a breach, the better off you will be.



01 Hackers Playground: The Metaverse and Augmented Reality

PREDICTION

Ready or not, the metaverse is here – and it is a hacker's playground. While embarking on a virtual life journey is an appealing concept to many, it is one rife with privacy and security concerns. As the metaverse continues to gain momentum, an onslaught of phishing attempts, NFT-related scams and malware attacks are looming. The use of AR and VR devices and technology increases the impact of data breaches as these devices collect large amounts of personal information and data from users, increasing their potential to be hacked and improving the sophistication of attacks.

A virtual world that offers on-demand immersive experiences, stunning visuals, entertainment, community, and new ways to connect and collaborate, the metaverse is bringing our online experiences to life in 3D. Gartner predicted that 25% of the population will spend at least an hour a day in the metaverse by 2026. Yet, as consumers and businesses figure out how to play, shop, work, and interact in this nascent universe, hackers already well-versed in digital ecosystems are finding ways to exploit its vulnerabilities.

Arkose Labs, an online account security and fraud prevention company, reported that in 2021, metaverse businesses faced 80% more bot attacks and 40% more human attacks than other businesses.

It's not just businesses that are at risk for cyberattacks in the metaverse. A NortonLifeLock survey of U.S. adults revealed 84% have at least some concerns about the metaverse, and 52% report having data concerns specifically, including breaches that would expose their personal information (40%) and lack of data privacy (39%). They're right to be wary.

In the same way that hackers can gain access to personal or corporate correspondence when they hack email accounts via phishing, malware, or credential stuffing, they can also gain access to personal data stored on an individual's preferred metaverse platform. Engaging in the metaverse requires more gear, such as VR headsets and AR glasses. Like phones, cameras, speakers and other smart devices, these present additional points of entry for hackers and thus, the probability of a data breach.

These devices are also constantly gathering information about users' movements, habits and preferences. They can record what a user looks and sounds like. Who has access to that data and how might they use it? A lack of comprehensive regulations regarding data capture and use in the metaverse isn't helping the situation. When that data is combined with other personally identifiable information, it has the potential to deepen the impacts of a hack.

NFTs (Non-Fungible Tokens), the epicenter of the metaverse economy, also pose a risk as cybercriminals sell fake NFTs or gain access to user funds and data through phishing scams. Crypto compliance company Elliptic reported that NFTs worth more than $100 million were stolen in the past year.

THE TAKEAWAY:

As more users enter the metaverse, the potential for victimization rises. A combination of savvy hackers already well-versed in digital ecosystems and a broader lack of regulations means critical user data is at risk for exposure. Proceed with caution into the virtual universe and remember that the security rules of the 2D online world still apply and are as critical as ever. Avatars in the metaverse may not be the people they want you to think they are.

02 Psst... Hackers Use AI, Too

PREDICTION

AI is a buzzword in every industry from healthcare to retail, so it's catching the attention of cybercriminals, too. 2023 is likely to bring an increase in AI-driven cyberattacks, and AI will be used as a key entry point to systems as bad actors exploit it for their benefit.

Organizations are utilizing AI in a vast number of ways for positive outcomes. Anyone who has ever bought a product on the internet has likely experienced AI-powered chatbots, many of which interact with a degree of competence and sophistication that emulates normal conversation. While capabilities vary broadly, AI can already reliably solve problems that normally require human intelligence. The most sophisticated systems operate on artificial neural networks – programs that mimic the human brain.

As much as AI is used for improved operations and processes, cybercriminals are lurking in the shadows to use it, too. Hackers have already successfully employed AI-driven cyberattacks, including on TaskRabbit in 2018. Hackers are using AI to create credible-looking phishing emails and believable audio and video files. In the face of rapidly advancing technology in space, we predict hackers will increasingly employ AI assistance in the year ahead, targeting more people with better defenses in less time. And, as evidenced by a recent controversy at Google that saw an engineer working on its AI chatbot fired for inaccurately claiming it was sentient, even the savviest minds in the industry are susceptible to deception.

A VentureBeat article citing executives from cybersecurity company Darktrace notes that phishing and spam are only the "tip of the iceberg when it comes to AI-powered cyberattacks." Other means can include augmenting malware with AI to sneak around systems undetected.

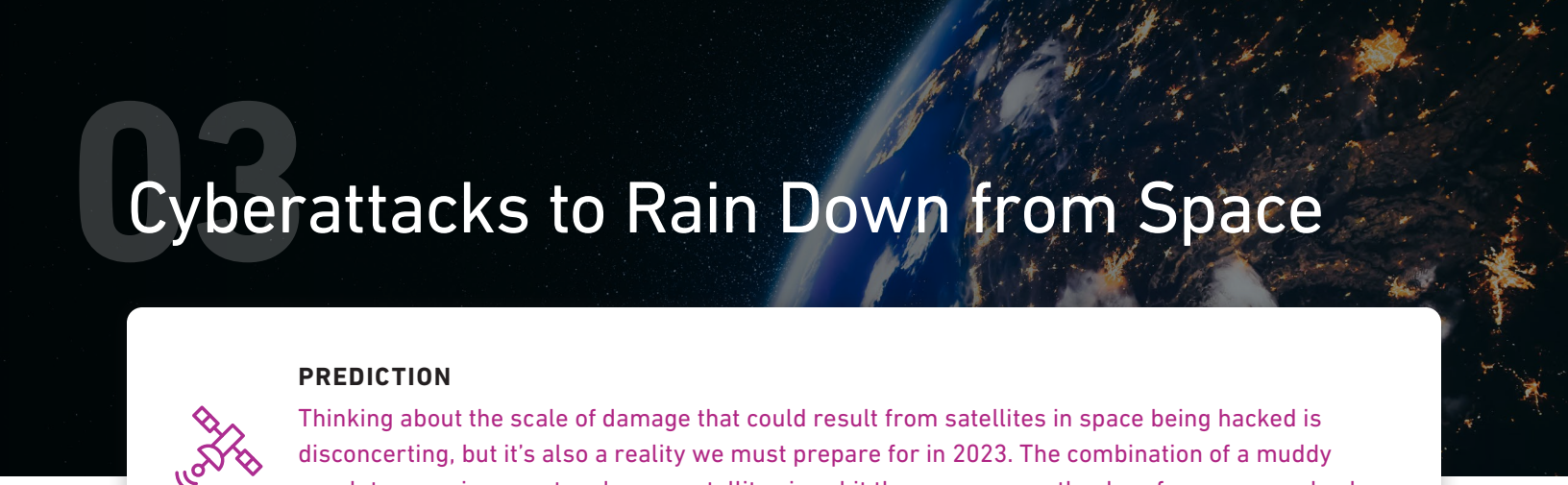
On the flip side, companies are using AI in their cybersecurity defense. A competent AI-based cybersecurity system is designed to recognize patterns and trends in data that could indicate an attack. It is intended to function independent of humans and process large amounts of data efficiently and objectively, but this also makes it vulnerable to poisoning. For example, Johannes Ullrich from SANS has proposed hackers could feed a system bad information to misguide it and have it learn to search for malware they will not actually use in their attack, thereby throwing the threat detection off course.

Bad actors also could use the information gathered by AI-based systems to carry out an attack. As Unite.ai points out, a system may identify points of weakness within the network. Ideally, the cybersecurity team would patch these and avoid a breach, unless a hacker, tipped off by AI, exploits the vulnerabilities first.

Finding vulnerabilities within an AI ecosystem and leveraging AI as an infiltration tool are both in the savvy cybercriminal's arsenal these days, meaning companies need to shore up security around their use of AI and AI systems in everyday operations. In a defensive posture, they will need to stay a step ahead in recognizing the security walls that bad actors can circumvent. In the wrong hands, AI's capacity to be weaponized becomes an ever-present threat.

THE TAKEAWAY:

Once the far-fetched material of sci-fi novels and films, the gaps and threats weaponized AI present are real, and cybercriminals are becoming more skilled at exploiting them. It's a virtual chess match bad actors are playing with increasing sophistication. Knowing the preferred means of attack are AI-powered phishing emails that are targeted and personalized, organizations can protect themselves by deploying a "zero-trust" model and staying vigilant of web traffic.



03 Cyberattacks to Rain Down from Space

PREDICTION

Thinking about the scale of damage that could result from satellites in space being hacked is disconcerting, but it's also a reality we must prepare for in 2023. The combination of a muddy regulatory environment and more satellites in orbit than ever opens the door for any savvy hacker to exploit or with a big enough satellite dish to launch attacks from space.

Imagine that a tech start-up in the growing private satellite sector operates a constellation of low-Earth-orbit (LEO) satellites. Its system has an out-of-date security patch that a hacker uncovers and attempts to exploit. If the company's cybersecurity defenses aren't resilient, that bad actor may be able to hack the company's entire satellite fleet and access all the data being transmitted to and from the satellites. They could jam up signals and cripple business operations, making life on the ground challenging for anyone dependent on the organization's infrastructure and services. There also are concerns about what the hackers might do with any uncrypted proprietary or personal data they intercepted.

Society's increasing reliance on satellite-dependent technologies brings with it a level of cyber risk that hasn't existed previously. There are more than 4,500 active satellites in orbit now, with thousands more planned. The sheer increase in the number of small satellites being launched means there will be more targets for cybercriminals to breach, increasing the potential of an attack.

Legacy satellites are not updated easily or regularly with patches and other security fixes, leaving them vulnerable to attack. There are also decommissioned satellites long forgotten and orbiting in space that can be hacked if bad actors have the means to reach them.

No system is immune to being compromised and security researchers have proven that this type of attack is possible with enough knowledge of existing systems and the proper signal amplification. In a 2020 Def Con Safe Mode Talk, a researcher demonstrated how it is possible for bad actors, using $300 worth of widely available home television equipment, to intercept sensitive data transmitted on satellite links by some of the world's largest organizations.

There also is the risk that satellites could be used as weapons. According to William Akoto, a professor at Fordham University, some satellites feature thrusters that allow them to accelerate and change direction in space. Akoto warns that these satellites could be used as weapons if hackers took control of them, noting they "could alter the satellites' orbits and crash them into other satellites, or even the International Space Station." In a space as unregulated as space, satellites could present a potent cybersecurity threat.

THE TAKEAWAY:

It is critical for governments and companies deploying assets into space to understand the cyber risks their systems present and how those inherent vulnerabilities could potentially be exploited by hackers. As we were writing this paper in November, there were reports of cyberattacks by Russia against communications and geospatial imaging platforms based in low Earth orbit that has been vital to Ukrainian defense. We foresee many nations and hackers exploring this landscape in the future so defenses must be shored up. You don't want Houston calling you with a problem.

04 Conflicts Caused by Weaponized Likenesses

PREDICTION

Global leaders, business titans and influential industry experts around the world can move markets and cause chaos with just a few pointed words. But what if these leaders could have their likeness weaponized? Anyone with widespread influence will need to be vigilant about protecting their image and likenesses as deepfake technology can be leveraged to cause chaos on both small and global scales.

In the war on misinformation, content is a powerful weapon. With "fake news" running rampant, it has never been more difficult to discern between what is real and what is fake.

The other war we are fighting is against cyberattacks on our information systems by nation-state actors and cybercriminals. These are grave threats in their own right, but the rise of deepfakes has enabled a new social engineering attack.

In the early stages of Russia's invasion of Ukraine, deepfake videos of both countries' leaders announcing a peace deal were shared widely on social media. While the videos were quickly identified as deepfakes and labeled as manipulated media by social media platforms, this incident serves as a stark indicator of how prominent figures can have their image and likeness manipulated by bad actors to serve different interests.

Deepfake-enabled attacks aren't only a tactic employed by nation-states. According to cybersecurity firm Trend Micro, "the growing appearance of deepfake attacks is significantly reshaping the threat landscape for organizations, financial institutions, celebrities… even ordinary people. The use of deepfakes brings attacks such as business email compromise and identity verification bypassing to new levels."

Consider the instance in Hong Kong in 2020 when a bank manager received a call from a person he believed was someone he knew and had worked with previously. The manager recognized the caller's voice and thought his verbal request for a $35 million transfer to support an acquisition and the subsequent supporting emails he sent were legitimate. In reality, the voice was a deepfake and the emails were bogus.

Expect potentially more scams like this in 2023 as remote work and virtual communications sustains their popularity across industries, even possibly among the everyday work and virtual communications. There have even been reports of bad actors using deepfake videos in online job interviews to secure remote work positions. Once they gain employment and access to an organization's network, they can steal data and wreak havoc.

VMWare reports that deepfake-enabled attacks are increasing rapidly. In a recent survey, 66% of respondents reported witnessing such attacks in the past 12 months, up from 13% in 2021.

THE TAKEAWAY:

Deepfake attacks on organizations will be effective in the short-term because companies are not fully aware of these threats yet and there are currently no mainstream technological tools available to detect and deter these types of attacks. Corporate leaders, celebrities, legislators and other high-profile individuals should be aware their likenesses could be used for malintent in the wrong hands.

05 Wars Will Have Two Battlefields: On the Ground and in Cyberspace

PREDICTION

The impact of the digital battleground as a tool of war is growing exponentially and may soon be as instrumental in the outcome of conflicts as much as soldiers on the battlefield. Cyberwarfare will be a part of the overall strategy and nations will look to ramp up their recruitment of cyber talent to keep up with their enemies.

Cyberattacks have long been a tool in nations' broader surveillance and weapons arsenals. However, we have seen for the first time that cyberwarfare may be as important as boots on the ground. There were reports of several cyberattacks before any physical attack in the conflict abroad this year including on a satellite company to disable communications. Tactics even spilled over to affecting civilians, with news of fake text messages being delivered to the targeted nation's residents saying ATMs in the country did not work.

We expect cyberwarfare to continue to gain prominence and be instrumental in military operations moving forward. In fact, Vectra AI CEO said, "we have long theorized that cyberattacks are going to be part of any nation-state's arsenal and I think what we're witnessing for the first time frankly in human history is cyberattacks have become the weapon of first strike."

To compete in this evolving battleground, we'll need not only to invest in technologies but also manpower. Currently, there are about 700,000 unfilled cybersecurity roles in the private sector.

In the military, it was reported that the United States Army will double the size of its active-duty cyber forces to approximately 6,000 by the end of the decade. With that, the branch is said to have asked for about $16 million in cyber and IT funding for next year. In other parts of the government, it was reported that the Pentagon received approximately $11 billion in cyber funding for 2023.

Based on what we've already seen, cyberwarfare will not only impact foreign and domestic soil. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued an alert for organizations, industry executives, and cyber experts on the attacks expected in 2023 and how to safeguard from potential targets.

THE TAKEAWAY:

In a news article, a director for the Defense Intelligence Agency said cyberwarfare is keeping him up at night. Rightly so, it's much easier to strike virtually. In our new world, an enemy can attack without ever leaving their desks. We expect to see much more cyber activity in global conflicts, and cyber-related jobs in the U.S. military to boom. Every branch has positions, according to a 2021 statement by the U.S. Cyber Command.

9 Years and Counting:

The Last Decade's Hits and Misses

To commemorate our 10th annual Data Breach Industry Forecast, we're taking a look back at the past nine years' worth of predictions to see how they fared. These are some of our top hits and misses.

The Hits

2014

Healthcare Breaches: Opening the Floodgates

We anticipated that the healthcare sector would be a major target back in 2014 and it was – one breach alone exposed the medical records of 4.5 million patients at 206 hospitals across 23 states. Overall, the healthcare industry accounted for 42% of major data breaches reported in 2014, according to the Identity Theft Resource Center.

The healthcare industry remains one of the most targeted sectors for cybercriminals. In 2021, breaches hit an all-time high with 45 million people affected, according to cybersecurity company Critical Insights. In the first half of 2022 alone, 337 breaches affecting 19 million medical records had already occurred, per data from Fortified Health Security's mid-year report.

2015

Missing the Mark: Employees Will Be Companies' Biggest Threat

Employees have been and continue to be the weakest link in an organization's security defense. In 2015, a report from the Ponemon Institute indicated the leading cause of data security breaches resulted from non-malicious employee error. According to Verizon's 2022 Data Breach Investigations Report, 82% of data breaches involved a human element. It comes as no surprise as cybercriminals have unleashed an onslaught of phishing emails and deployed new technology to target employees, gain access to their credentials and infiltrate systems.

2016

The EMV Chip and PIN Liability Shift Won't Stop Breaches

We continued to see payment breaches across all sectors in 2016. Through malware-driven attacks on restaurants like Wendy's and the Oracle MICROS breach, we learned while EMV may make payments more secure, it will not stop breaches from occurring altogether due to system sophistication and weak spots in payment processes. Credit card fraud remains a significant issue, one reason being that merchants continue to use mag stripes. Consumers and businesses will need to continue to be vigilant when using credit cards; as the pandemic eased in 2021, there was an almost 40% increase in point-of-sale attacks, according to a report by Kaspersky.

9 Years and Counting:

The Last Decade's Hits and Misses

To commemorate our 10th annual Data Breach Industry Forecast, we're taking a look back at the past nine years' worth of predictions to see how they fared. These are some of our top hits and misses.

The Hits -Continued

2016

Presidential Candidates and Campaigns Will Be Attractive Targets for Hackers

The 2016 presidential race proved pivotal in how campaigns would be handled from a cybersecurity perspective. Unfortunately, our prediction proved correct when Russian hackers gained access to the Democratic National Committee servers and stole information.

Fast-forward to this year with the mid-term elections upon us as we write this paper, it was reported that the FBI warned both parties of potential targeting by Chinese hackers. Elections will always be attractive to hackers, whether to incite chaos or manipulate the U.S. democratic process.

2019

Friends or Foes in Online Gaming

It wasn't game over, but 2019 saw its fair share of cybercriminal activity in the online gaming world. Retro gaming platform Emuparadise revealed a breach that exposed the account information of more than 1 million users, and hackers declared a cyberwar on gamers via a DDoS attack on video game developer Blizzard Entertainment servers during the highly anticipated release of its World of Warcraft Classic game.

There has been no slowdown in this industry – in April 2022, a report by Akamai Technologies noted cyberattacks targeting the gaming industry grew by more than 100% in the last year. A senior executive told Silicon Republic, "As gaming activity has increased and evolved, so has the value of disrupting it through cyberattacks."

2021

Vaccine Ripple Effect

The pandemic's impact was evident in our predictions in 2021. Like with any global or societal issue, bad actors were waiting in the wings to determine how to leverage it, leading us to predict that hackers would plot to disrupt vaccine supply chains and infiltrate the distribution ecosystem. In April 2021, IBM reported that its cybersecurity unit uncovered an increase in attacks targeting the global COVID-19 vaccine supply chain since originally flagging the threat during initial rollout in late 2020.

These attacks were widespread and global in nature: Oxford University's COVID-19 vaccine researchers faced an attempted ransomware attack; hackers compromised the IT systems of a vaccine scheduling app in Italy; and the Brazilian Ministry suffered an attack that eliminated its COVID-19 vaccination data. The list goes on and on.

9 Years and Counting:

The Last Decade's Hits and Misses

To commemorate our 10th annual Data Breach Industry Forecast, we're taking a look back at the past nine years' worth of predictions to see how they fared. These are some of our top hits and misses.

The Misses

2016

Hacktivism Makes a Comeback

Hacktivisim continued throughout 2016; however, its resurgence was not as prominent as predicted. While hacks against ISIS did amount to some coverage, hacktivist efforts have generally not had the same impact as in years past. Of note, Anonymous continued to target international banks and governments with DDoS attacks.

2017

U.S. Critical Infrastructure Will Be Subject to a Disruptive, Large-Scale Attack

We were a little ahead of our time, as this prediction didn't come true in 2017, but rather in 2020 and again in 2021. In 2018, a handful of smaller-scale attacks did occur when hackers targeted hundreds of U.S. companies across various critical infrastructure sectors, including electric power utilities and nuclear plants. Several were compromised, according to the Department of Homeland Security. However, no major cyberattacks occurred until 2021, most notably when the Colonial Pipeline was compromised by ransomware, causing significant supply issues across the U.S. According to the latest Microsoft Digital Defense Report, cyberattacks on critical infrastructure accounted for 40% of all nation-state attacks over the past year, up from 20% the year prior.

2020

Hackers in the Sky with Data

As free public Wi-Fi becomes more readily available across the globe, consumer data that passes along on unsecured networks is left exposed in the digital and physical clouds above. We predicted that hackers would deploy drones to steal data from devices connected to public networks. This notion may have raised eyebrows, yet we didn't see major activity in 2020. In 2022, however, a U.S. financial firm specializing in private investments experienced a cyberattack of this nature. After detecting unusual activity, the company found two modified DJI drones on the roof of its building, one of which was carrying a modified Wi-Fi Pineapple device that was spoofing the Wi-Fi network that employees normally connect to.

According to BlackBerry researcher Dmitry Bestuzhev, drone-powered attacks should not surprise us: "Drone attacks are a new standard. They have been active assets in real-life conflicts and are now part of the cyberattack surface."