Experian® 2021 Data Breach Industry Forecast

experian™

Executive Summary

2020 was a year of change and uncertainty. This made for a prosperous climate among cybercriminals. While nations scrambled to mitigate the COVID-19 pandemic, cybercriminals found new opportunities to strike. As businesses and citizens adjust to a "new normal," hackers have likewise honed in on new targets and new means to access sensitive data certain to wreak havoc in the New Year.

Powerful under the veil of a crisis, tech-savvy hackers found the perfect opportunity to steal data from our smart devices, contact tracing applications, rural hospitals, and frenzied clinics. The application of new technologies to aid our response to the pandemic have also opened up new threat vectors that in many cases, have yet to be safeguarded. In South Dakota, for instance, an online portal was built early in the year to help first responders identify people who had tested positive for COVID-19. Now, the FBI is investigating a June data breach that exposed the names, addresses, birthdates, and health status of those individuals it intended to help.[1] The result: patient confidentiality was undermined.

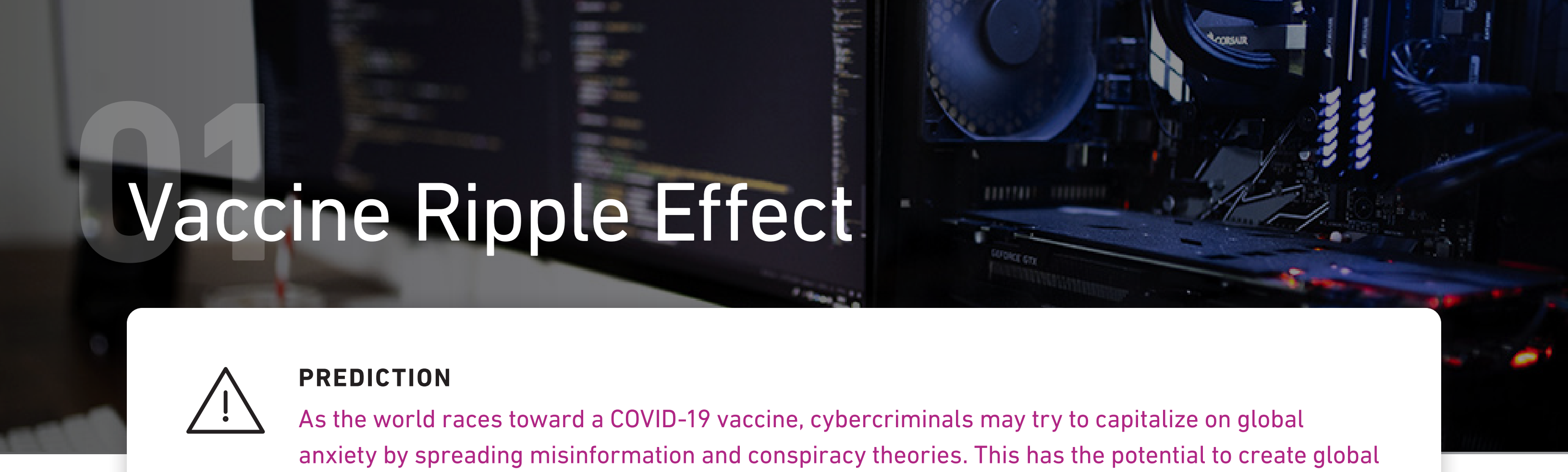
"Social distancing," an unfamiliar term only a year ago, will continue to be part of our norm in the year to come. Companies have had to quickly navigate the changes brought about by social distancing guidelines and adapt to remote working environments, with cybersecurity looming as an afterthought. With more information being shared across devices and services, businesses must double down on data protection and security to protect against these emergent risks.

In the Eighth Annual Edition of Experian's Data Breach Industry Forecast, we examine some of the areas that have become increasingly vulnerable to cyberattack amid the COVID-19 era. We also outline five predictions for the data breach industry in 2021.

The predictions by Experian Data Breach Resolution are rooted in Experian's long history of helping companies navigate more than 50,000 breaches over the past 17 years.

Based on our expertise, the top data breach trends of 2021 include the following:

- Much of 2020 has been spent racing for a COVID-19 vaccine, which is providing an opportunity for cybercriminals to strike. We predict that these intruders will plot to disrupt vaccine supply chains, sow confusion and spur increased national competition, creating a new kind of pandemic warfare.
- While working from home was nothing new, a mass transition to remote work provided hackers with a wealth of network targets through connected household devices. Attacks are getting smarter and more dangerous, and many families are unprepared for this onslaught in the coming year.
- Contact tracing apps were created to help flatten the curve of COVID-19. However, many don't employ sufficient security protection, making these new tools a boon for hackers looking to steal shared data in 2021.
- Faster doesn't always mean safer. High-speed 5G will usher in amazing new possibilities, but with those advancements come increased vulnerabilities and risk. These risks are magnified as billions of connected devices, vehicles and sensors increase the surface area for attack. As a result, cybercriminals will certainly find ways to gain access to 5G networks to cause chaos with our cell phones, autonomous vehicles, health records and more.
- More breaches involving personal medical information may be on the horizon. Much of this risk will come as healthcare providers rushed to adopt digital and telehealth services and patients become more comfortable with leveraging technology for healthcare services.



01 Vaccine Ripple Effect

PREDICTION

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.

This year we have a two-fold prediction. First, social media will be a playground for anti-vaccination rhetoric, which started infiltrating months before COVID-19 vaccine discussions began. Social media companies have been taking major steps in tackling misinformation from fake accounts and coordinated groups churning out disinformation. But there's a blurred line between misinformation and free speech, which will continue to be defined in 2021.

Many will keep a watchful eye for information that surrounds a vaccine rollout. Some people might be willing to make rash or irrational decisions for vaccine access. Others will be suspicious of the intentions behind the vaccine's fast-paced development. Both are targets for cybercriminals, who have the ability to manipulate and cause chaos through false rumors and misinformation.

As far back as May 2020, Facebook stated it had already removed hundreds of thousands of posts that violated its COVID-19 policies. It put "warning labels" on about 50 million more.[2] The year wasn't even halfway over.

It turns out this misinformation isn't just harmful for our society; it's expensive. Advertising-fraud cybersecurity firm CHEQ estimates $78 billion is lost to it annually. It further estimated that health misinformation in particular led to $9 billion in unnecessary healthcare costs and other expenditures.

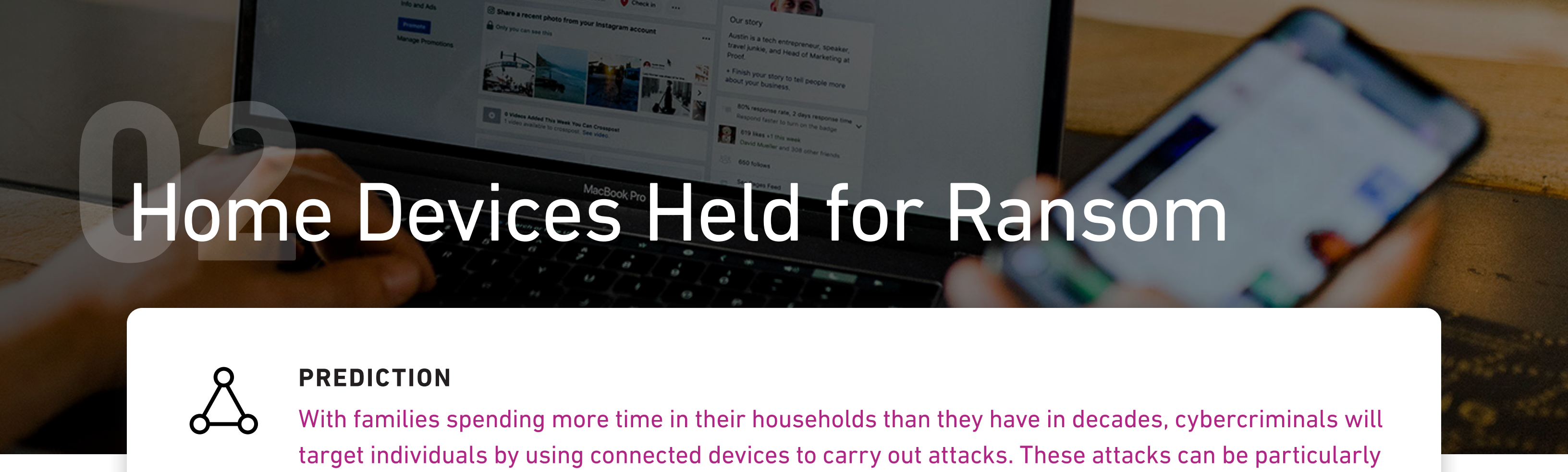
As the vaccine rollout begins, our second part of this prediction is that cyberattacks like these provide cybercriminals with the potential to bring harm to supplies, supply chains, and cargo shipments, severely disrupting and delaying government response efforts.

When a COVID-19 vaccine becomes available, global leaders will need to make important decisions about its transport and the first recipients. Throughout 2020, hackers from around the world were targeting the vaccine itself. For instance, the U.S. Department of Justice accused individuals from China of attacking vaccine development and supply chains on behalf of its intelligence service.[3] It's possible this hack was part of a broader campaign of global cybertheft aimed at industries such as defense contractors, high-end manufacturing, and solar energy companies. Hackers from Russia were accused of attacking COVID-19 vaccine research. American, British, and Canadian governments accused the Kremlin, Russia's executive branch, of opening a new front in its covert operations against the West amid the worldwide competition to contain the pandemic.[4]

According to the 2020 Supply Chain Resilience Report from global manufacturing network 3D Hubs, 72% of companies have experienced disruptions to their manufacturing supply chain in the past decade, with pandemics, natural disasters, and trade wars being the most common disruptions.[5] Unsurprisingly, the COVID-19 pandemic has been the single greatest disruptive event in the past decade, with 60% of companies stating the virus disrupted their manufacturing supply chain.

THE TAKEAWAY:

Social media is a source of information for people around the world. As we enter 2021, we'll likely see anti-vaccination rhetoric and medical misinformation reach new highs, sowing social discord and global chaos. When you read or see inflammatory information, be diligent in researching the source. You should remain vigilant in evaluating the information you are exposed to and see on social media. If it's from a questionable source, do more research to ensure you're not falling prey to a false information attack. For any organizations involved in the vaccine distribution ecosystem, amp up your cybersecurity.



02 Home Devices Held for Ransom

PREDICTION

With families spending more time in their households 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.

In the past, cybercriminals targeted organizations over individual households. However, the recent transition to remote work has been a gift to hackers looking to gain access to sensitive information and use it to extract cash from unsuspecting individuals.

People have adapted to working, going to school, and hosting family and social gatherings entirely on their connected devices. Cybercriminals see an opportunity to target these individuals, especially those making a sizeable income. High-income individuals and celebrities are not only easier for hackers to search for online due to their often-public persona, but also are more attractive targets because of their ability to pay ransom. In fact, according to research by UK-based Campden Wealth, 28% of ultra-high-net-worth individuals have been a victim of one or more cyberattacks, yet over a third of those surveyed reported having no cybersecurity plan in place.[6]

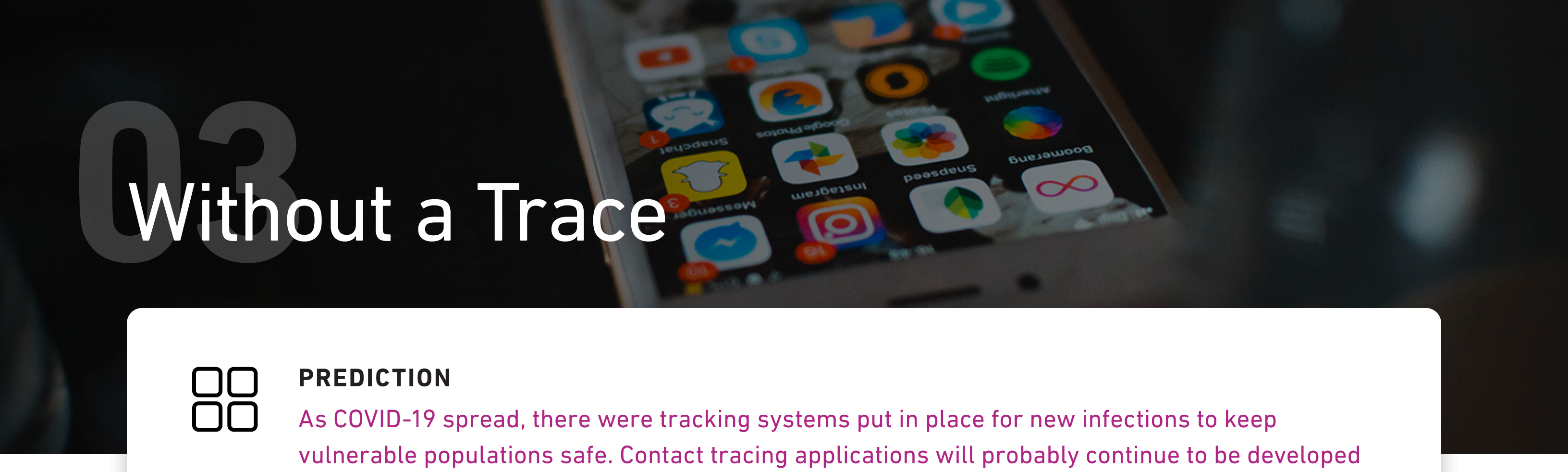
Ransomware, a type of malicious software, can commonly occur when threats to lockdown or publish a victim's data are used to extrapolate money. While ransomware attacks aren't new, they are getting smarter and more sophisticated. In July 2020, hackers took to one of the most popular social media sites, Twitter, to virtually hold approximately 130 celebrities, influencers, and political leaders hostage by making false promises to double bitcoin deposits. As a result, the scammers were able to extract more than $100,000 in cryptocurrency.[7]

Ransomware attacks thrived in the first half of 2020, increasing by 72% according to an analysis of malicious activity published in Skybox Security's 2020 Vulnerability and Threat Trends Report.[8] A transition to targeting the rich and famous and possibly, even simply, vulnerable families will be the next iteration of these attacks.

With control over home devices, doors, windows, and security systems, cybercriminals have the potential to hold an entire house hostage in exchange for money, information, or even fame. In the coming year, it's important to be aware of the possibility of home cyberattacks and prepared in the event that one occurs.

THE TAKEAWAY:

Whether you love it or hate it, working from home will most likely be a big part of 2021. Many people aren't prepared for the data security challenges that come with this trend, giving hackers a window of opportunity to do their worst. And while smart homes offer convenience and ease, they might not be so smart with the data you entrust to them. If possible, restrict device access or turn them off entirely when not in use. Be sure to monitor your devices when in use and evaluate security technologies to safeguard your connected home. Taking these actions, along with always keeping your home's data security in mind, could help prevent you and your family from becoming the next victim of a cyberattack.



03 Without a Trace

PREDICTION

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.

Contact tracing apps are a double-edged sword. Widespread adoption of contact tracing apps could help us minimize the spread of COVID-19, but these systems also have the potential to leave us vulnerable to cyberattacks—exposing the private information of thousands of people. Oxford University researchers said as much as 60% of a population would need to install and use a contact tracing app to effectively slow the spread of COVID-19.[9] Without proper security measures in place, over half a country's population would have data ripe for a cyberhacker's picking.

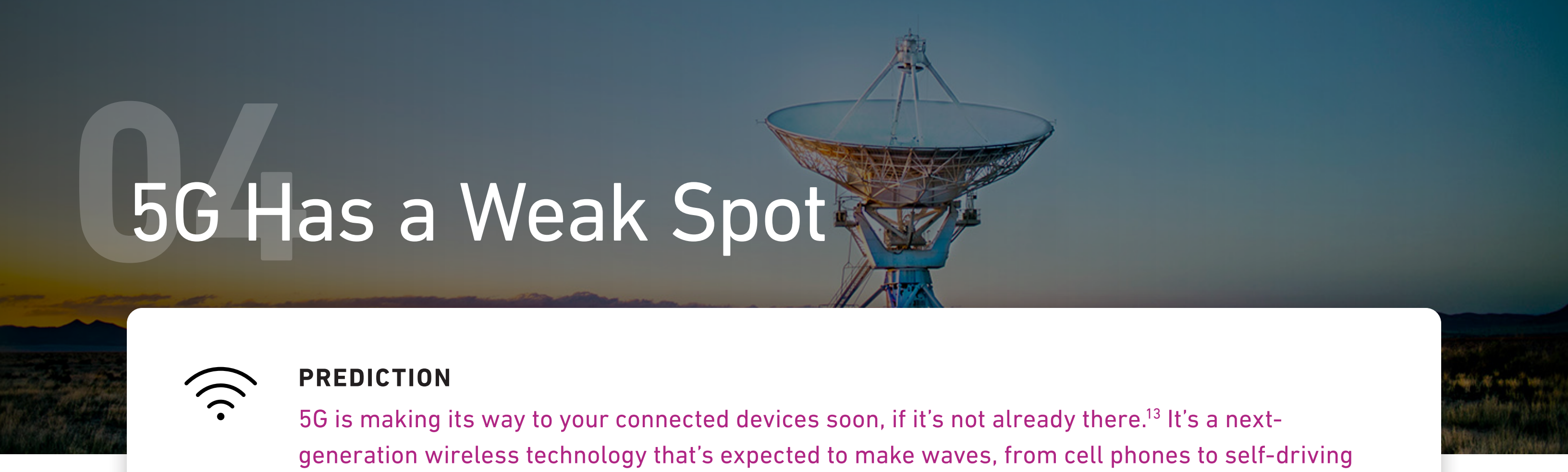
According to a report from Guardsquare, most government COVID-19 contact tracing apps don't employ sufficient security protections. The report found most of these apps make it easy for hackers to decompile, attack, and even create fake clones of legitimate contact tracing apps.[10]

How do contact tracing hackers work? Besides finding vulnerabilities in the networks and swiping information directly, they pretend to be contact tracers themselves and employ tactics such as sending fake text messages to users. Of course, this is all a ploy to trick users into giving up personal information or opening up access to their email or bank account information.[11] Hackers may attempt to access information through embedded text message links. By clicking on these links, victims may be downloading malware onto their devices without knowing it. This gives hackers access to personal and financial information without the victim's knowledge.[7]

It isn't just cybercriminals looking to break into these networks. Digital activists, or "hacktivists," are another type of hacker to look out for in 2021. They can be especially active in areas of civil unrest or situations involving injustice. According to Politico, hacktivists may be motivated to take down contact tracing apps in an effort to gain notoriety. They may also use identity information obtained by contact tracing apps as a hidden surveillance tool, or even worse, for cyber espionage.[12]

THE TAKEAWAY:

Contact tracing apps, a source for good in the fight against COVID-19, have a downside. Consumers should do their due diligence to make sure they stay safe from hackers and scammers in this new frontier. Check to see if your phone carrier can help you block numbers from unknown senders. Utilize call-blocking apps that weed out unidentified senders. Enabling multi-factor authentication on your device will provide an extra layer of protection from unknown assailants. The best way to avoid being a victim of a contact tracing scam? Don't click on strange or unfamiliar links. This a rule that should be followed at all times, whether you participate in contact tracing or not.



04 5G Has a Weak Spot

PREDICTION

5G is making its way to your connected devices soon, if it's not already there.[13] 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.

While there are a number of benefits that come with the implementation of 5G networks, we believe the technologies relying on it may be vulnerable to cyberattacks in 2021. 5G is designed to support a 100x increase in traffic capacity and network efficiency.[14] What makes 5G implementation concerning is its predicted use in the automobile and healthcare industries, which require specific security requirements — as well as the public's trust.

For example, the advent of 5G networks is poised to unleash a caravan of self-driving vehicles on the roads. This provides hackers with the potential to manipulate signals, cause accidents, and disrupt the logistic chains we rely on. The speed at which communications go back and forth between servers and vehicles make these cars highly vulnerable to cyberattacks, where even a momentary disruption can put lives at risk.

In healthcare, 5G is expected to revolutionize telehealth with its quick speeds and ability to transport data.[15] A single patient can generate hundreds of gigabytes of data in a given day; these include patient medical records and large image files such as MRI, CAT, and PET scans. 5G can also be used to provide medical gadgets to patients, who can then monitor and measure their health from home.

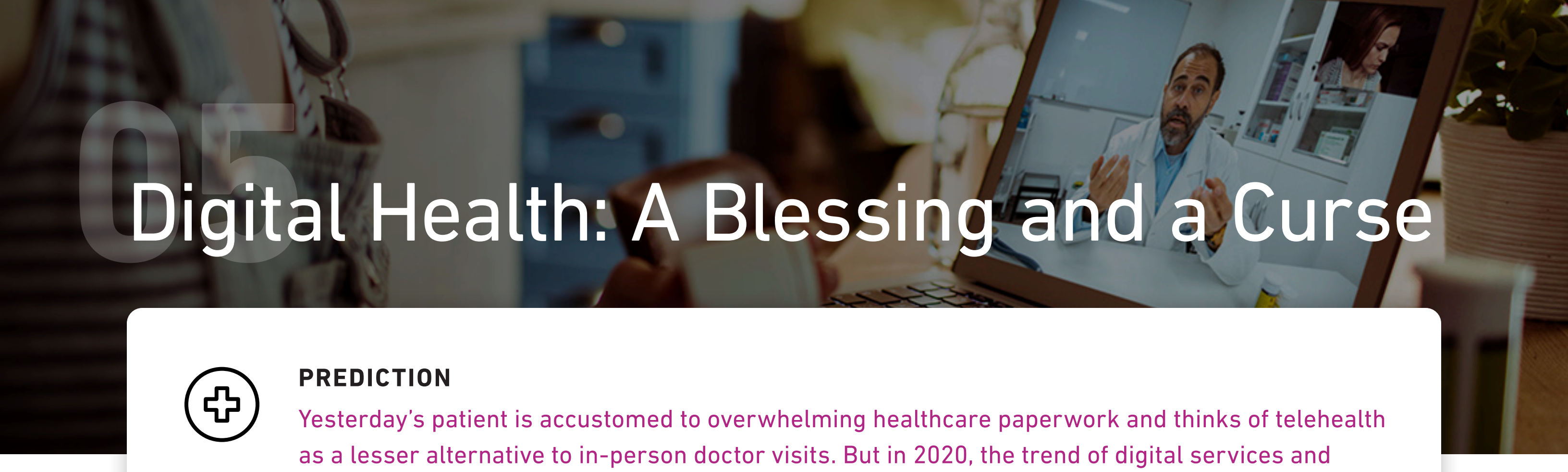
While this advancement is great for our everyday lives, it may come at a high cost. We'll become more reliant on our electronic devices, giving cybercriminals new and creative ways to extract our personal information.

The proliferation of technologies embedded in our phones, cars, industrial controls and trusted institutions increases the potential of cyberattacks with the advent of 5G. The communication systems between devices and infrastructure present remote attack access for malicious hackers looking to exploit system vulnerabilities. Increased connectivity poses a considerable threat to the benefits promised by vehicles that can drive themselves, X-rays on demand, and lightning-fast cell-phone service.

Going forward, security organizations that rely on manual approaches may have a hard time keeping up with the speedy service of 5G. Digital security that is dynamic and automated will quickly and effectively address the new security threats of 5G networks, and virtualization can help provide flexibility to respond to unknown future threats.

THE TAKEAWAY:

Changes in technologies are on the way with the implementation of 5G. But like any other device that we rely upon, their connection to an always-on network leaves them open to cybercrimes and security threats, whether it's your cell phone, car or online healthcare portal. Be sure that your personal devices are restricted or off when not in use and be aware that "faster" may not always be the same as "better." A more connected world will require a keen focus on cybersecurity measures to keep us on the road to a bright future.



05 Digital Health: A Blessing and a Curse

PREDICTION

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.

The U.S. Department of Health and Human Services states the number of telehealth primary care visits increased 350 times in April 2020 compared to pre-pandemic levels.[16] With hospitals stretched to their limits, virtual visits became the practical means of receiving care at a safe distance.

As the telehealth field quickly evolves to become a regular part of doctor-patient relationships, cybercriminals are spotting an increasing opportunity. Personal and medical records have a high price tag that unlawful individuals can cash in on. In fact, a single record can go for anywhere from $250 to $1,000, according to Louis Columbus of Dassault Systemes.[17] This information could be exposed through new communication modes and as more healthcare institutions implement 5G technology (more on that later on).

Cyberattacks are nothing new to the healthcare industry. However, a rush to develop and implement telehealth technology and a host of other digital health services could make it even easier for cybercriminals looking to gain access to private medical records in the coming year.

In 2020, telehealth providers experienced a nearly exponential increase in targeted attacks as their popularity skyrocketed — including a 30% increase in cybersecurity findings per domain.[18]

Healthcare hackers tend to target older systems that lack sufficient security, which means small and underfunded clinics have traditionally been targets for breaches. These providers are particularly at risk as they navigate the world of telehealth, falling even further behind their peers as they hurry to adopt a system in 2021.

Patient privacy aside, a single breach in digital hospital records has the potential to shut a system or practice's entire network down for days. These attacks can also lead to a massive operations interruption, substantial fines, and the potential for lawsuits on behalf of patients who weren't able to receive care or whose information was exposed.

THE TAKEAWAY:

Healthcare organizations are evolving for the better offering patients' easier and faster ways to conduct business, but it will come at a price if entities don't pay attention to cybersecurity. Hospitals and clinics must continue to be vigilant in keeping their cybersecurity programs up-to-date and under regular review. While COVID-19 caught the world by surprise, 2021 provides organizations with an opportunity to focus on beefing up their cybersecurity programs. If you plan on using digital and telehealth services, protect yourself by practicing good security hygiene such as changing your passwords often and logging out of browsers immediately after your doctor visit has ended.

2020 Forecast Scorecard Ratings

A+

Phishing 2020

Cybercriminals' latest tool in their belts is text-based "smishing," an identity theft technique targeting online communities like those around presidential candidates. Fraudulent messages disguised as fundraising communications are harder to ignore, distinguish, and take advantage of consumers in a contentious election cycle.

UPDATE

Millions of cell phone users have recently received unsolicited text messages, alleging they have an unclaimed package for them. The texts include a link that often sends the user to a fake Amazon website asking for personal information and usually ends up in identity theft. According to the Better Business Bureau, another scam uses the COVID-19 pandemic to target people through text messages that encourage people to claim emergency money for groceries due to the coronavirus outbreak.[19]

B

Hacker in the Sky with Data

With more states installing free public WiFi on city streets, consumer data passing along on unsecured networks are exposed in the clouds above – digital and physical. Hackers are deploying drones to steal data from devices connected to public networks.

UPDATE

According to recent research by France-based Synacktiv and the U.S.-based GRIMM, an Android application used to operate drones manufactured by DJI contains several abusive features.[20] These drones could allow cybercriminals to attack users with malicious applications or fully take over control of users' cell phones. RAND, a nonprofit global policy think tank, identified an example in which a drone flies over a specific area, such as city streets, collecting information on the WiFi area's networks. The drone accessed vulnerable systems and connected devices on it to a botnet full of malware. Such infiltration can lead to distributed-denial-of-service (DDOS) attacks, stolen data, and hijacked devices. So maybe wait for that file to download over cellular data if you can.

A

It’s a Fake!

Less entertaining and far more problematic than TikTok videos, deepfake videos use advanced video and audio technology to create geopolitical confusion that can disrupt commercial enterprises, financial markets, and governments. These videos may seem real, but they are constructs of cybercriminals intent on sowing chaos.

UPDATE

Security consulting firm NISOS released a report analyzing an actual deepfake and shared the audio with Vice’s Motherboard website.[21] This deepfake came in the form of a voicemail. The deepfake, which was a voicemail sent to an employee at an unnamed tech firm, includes a voice that sounds like the company’s CEO asks the employee for “immediate assistance to finalize an urgent business deal.” Recognizing the need to combat deepfakes, Microsoft has expanded its suite of deepfake-spotting technologies and even launched a tool for analyzing videos and still photos that generates a manipulation score.[22] Even banks are beginning to work with financial technology to counter frauds, and since 2019 deepfakes have grown 20x.

A-

Going Up in Smoke

Online activism or “hacktivism” aims to disrupt more than Fortune 500 and blue-chip companies; emerging industries are also in cybercriminals’ sights. Cannabis retailers, cryptocurrency entities, and even environmental companies are becoming targets of digital protest.

UPDATE

We gave this one an A- because while there were fewer incidents than we thought there would be, this prediction did come true. For instance, according to researchers, a software company was impacted by a recent data breach, which led to the theft of tens of thousands of pieces of customer information from multiple U.S. marijuana dispensaries.[23] The stolen data included photo IDs, phone numbers, and home addresses – all left online without password protection late last year, according to experts from vpnMentor. The U.S. government also worked to seize control of 280 illegal cryptocurrency accounts. North Korea allegedly sponsored attackers in their efforts to hack cryptocurrencies and funnel $250 million in stolen money through a Chinese money-laundering network.[24]

C

Data Here, Get Your Data Here!

Mobile payments as a safer and seamless way to contactless purchase goods are popping up everywhere, and so is identity theft. Cybercriminals are exploiting the convenience in point-of-sale transactions from your local cafe to a stadium beer vendor, especially in larger venues like concerts and festivals.

UPDATE

Due to COVID-19, our prediction referring to large venues, concerts, and sporting events can’t be accurate. Despite national shutdowns, Landry’s, a popular U.S. restaurant chain, announced a malware attack on its point of sale (POS) systems that allowed cybercriminals to steal customers’ payment card information. In January, hackers sold the payment card details of more than 30 million Americans and over one million foreigners on Joker’s Stash, the internet’s largest carding fraud forum. We’ll wait while you google that site.

This hack was advertised under the name of BIGBADABOOM-III, but according to threat intelligence firm Gemini Advisory, the attack was committed via POS systems at Wawa, a convenience store chain based on the East Coast.[25]

About Experian Data Breach Solutions

Experian Data Breach Resolution, powered by the nation's largest credit bureau, is a leader in helping businesses prepare for a data breach and mitigate consumer risk following breach incidents. With more than a decade of experience, Experian Data Breach Resolution 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 theft protection products. Experian Data Breach Resolution is active with the International Association of Privacy Professionals, NetDiligence, Advisen, the Ponemon Institute RIM Council, and is a founding member of the Medical Identity Fraud Alliance.

For more information, visit Experian.com/DataBreach and follow us on Twitter @Experian_DBR.

SOURCES

1. https://apnews.com/article/cfdfc0b77303664b165faf4866887612
2. https://www.consumerreports.org/social-media/social-media-misinformation-policies/
3. https://www.nytimes.com/2020/09/16/us/politics/china-hackers.html
4. https://www.nytimes.com/2020/07/16/us/politics/vaccine-hacking-russia.html
5. https://www.3dhubs.com/get/supply-chain-resilience-report/
6. http://www.campdenresearch.com/content/private-confidential-cyber-security-report
7. https://www.justice.gov/usao-ndca/pr/three-individuals-charged-alleged-roles-twitter-hack
8. https://www.skyboxsecurity.com/blog/vulnerability-and-threat-trends-report-2020-key-findings/
9. https://www.cnbc.com/2020/07/03/why-coronavirus-contact-tracing-apps-havent-been-a-game-changer.html
10. https://www.guardsquare.com/en/blog/report-proliferation-covid-19-contact-tracing-apps-exposes-significant-security-risks
11. https://www.consumer.ftc.gov/articles/how-recognize-and-report-spam-text-messages#spam
12. https://www.politico.com/news/2020/07/06/coronavirus-tracking-app-hacking-348601
13. https://www.lifewire.com/5g-availability-us-4155914
14. https://www.qualcomm.com/invention/5g/what-is-5g
15. https://www.telit.com/blog/4-revolutionary-use-cases-5g-healthcare/
16. https://aspe.hhs.gov/pdf-report/medicare-beneficiary-use-telehealth
17. https://www.forbes.com/sites/louiscolumbus/2019/10/20/5-strategies-healthcare-providers-are-using-to-secure-networks/#665a5be4b40f
18. https://securityscorecard.com/resources/healthcare-industry-telehealth-cybersecurity-risks-report
19. https://www.whsv.com/content/news/Better-Business-Bureau-warns-of-coronavirus-text-message-scam-568904871.html
20. https://www.cyberscoop.com/dji-drones-china-android-application/
21. https://www.theverge.com/2020/7/27/21339898/deepfake-audio-voice-clone-scam-attempt-nisos
22. https://techcrunch.com/2020/09/02/microsoft-launches-a-deepfake-detector-tool-ahead-of-us-election/
23. https://www.newsweek.com/thsuite-data-breach-marijuana-dispensaries-personal-information-leaked-exposed-1483645
24. https://threatpost.com/doj-aims-to-seize-280-cryptocurrency-accounts-used-by-hackers/158757/
25. https://www.zdnet.com/article/wawa-card-breach-may-rank-as-one-of-the-biggest-of-all-times/