[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@2de591ea75ee4c899f4304d14e667254?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

**Reference**[**https://www.networkcomputing.com/careers-and-certifications/everything-vulnerable**](https://www.networkcomputing.com/careers-and-certifications/everything-vulnerable)

**Everything is vulnerable**

[Facebook](https://www.networkcomputing.com/#facebook) [Twitter](https://www.networkcomputing.com/#twitter) [LinkedIn](https://www.networkcomputing.com/#linkedin) [Reddit](https://www.networkcomputing.com/#reddit) [Email](https://www.networkcomputing.com/#email)It seems everything electronic these days is vulnerable to exploitation. And even though I'm on vacation, such vulnerabilities can't be ignored. Thanks to Tim Heagarty CISSP, MCSE for pointing out that our new Axis Network Camera was vulnerable in a...MAY 28, 2003

It seems everything electronic these days is vulnerable to exploitation. And even though I'm on vacation, such vulnerabilities can't be ignored.  
Thanks to Tim Heagarty CISSP, MCSE for pointing out that our new [Axis Network Camera](http://192.155.11.50/) was vulnerable in a nasty way. Seems that you could get around the HTTP Basic authentication and do things like change the administrative password on us. But thanks to Tim, I patched the Axis last night and all seems well.  
A new firmware upgrade was called for, and I have to say that Axis makes this a simple process. Simply ftp the new firmware to the device and, if you give it the right name, it automatically upgrades itself. Sweet.

reference <https://polyverse.com/blog/when-everything-is-smart-everything-is-vulnerable-bdc802694714/>

**When everything is “smart”, everything is vulnerable**



By Guest

It seems that every day brings a new gee-whiz innovation to consumer technology: [smart walls](https://www.theverge.com/circuitbreaker/2018/4/28/17289976/smart-wall-carnegie-mellon-disney-home) are the latest example setting tech blogs abuzz with speculation. The promise of smart walls is certainly interesting: a sensor built into any wall that turns it into a giant touchpad, capable of receiving commands to operate other “smart” areas of your home. One can easily imagine a future where such technologies infuse our homes, cars and businesses, automating the mundanities of daily life in ways we could scarcely have imagined a few years ago. The Internet of Things will increasingly be folded into the fabric of our reality. Life will be more convenient than ever before. But…

… we’ll also be a more *vulnerable* society than ever before.

Having a car, home or appliance that connects to the internet has many benefits, but it also exposes them to the same risks that your computers and phones already deal with: malware, spyware and hacking. The consequences could range from the merely annoying (a script that causes the lights in your home to flicker on and off) to the dangerous (a car hacked to lose control on the highway). These aren’t even hypothetical: numerous research projects demonstrate that the [possibility is already real](https://www.wired.com/2016/03/fbi-warns-car-hacking-real-risk/). Everything is hackable, but the present trend of rapid innovation means that developers of new technologies are often more focused on getting their ideas to market as soon as possible, rather than on getting them there *secure*.

Fortunately, logical security solutions are already adapting to anticipate and react to new threats before they can emerge. Merely detecting a problem and then patching/fixing it will hardly cut it in the situations described above?—?new security protocols must be *proactive* in nature, stopping attacks before they can begin. [Moving Target Defense](https://www.dhs.gov/science-and-technology/csd-mtd), or MTD, is an exciting development in this space, offering a new approach to data protection that eschews traditional infrastructure-based methods of “detect and quarantine” in favor of utilizing techniques such as system randomization, dynamic networking, and dynamic compilation to create an adaptable defense layer that swiftly renders moot almost any given method of attack.

MTD is one of several sophisticated solutions to a problem that grows ever more complex as more of our daily technologies depend on the cloud. But how do you keep your systems safe without having to learn the increasingly complicated ins-and-outs of modern logical security? After all, you don’t want to be in the security business just to run your own business. This is where automation comes in, keeping your environment secure and updated around-the-clock without any extra overhead (or headache) on your part. Significant strides have been made in automating secure cloud environments, prompting more and more businesses to manage their data in stress-tested and compliance-audited cloud services such as Azure, rather than reinventing the security wheel by themselves.

Technologies such as MTD are not passing trends designed to generate more clicks on security blogs. As cybersecurity predictions in 2018 promise more sophisticated logical threats from, for example, [AI-powered and state-sponsored networks](https://www.csoonline.com/article/3250086/data-protection/7-cybersecurity-trends-to-watch-out-for-in-2018.html), they will prove fundamental in keeping our data secure. It’s an unfortunate truth of the industry that logical security is locked in an endlessly escalating arms race with attackers, as each hopes to stay ahead of the other by leveraging the innovations of the day. Which means that whether you’re a consumer or an entrepreneur, you should ask yourself: are you moving to get ahead of these new threats, or are you standing still?

Reference <https://www.cmswire.com/cms/customer-experience/high-profile-hacks-prove-everyone-and-everything-is-vulnerable-019755.php>

**High Profile Hacks Prove Everyone and Everything is Vulnerable**



By [Dan Berthiaume](https://www.cmswire.com/author/dan-berthiaume/) | *Feb 22, 2013*

Hacking has been all over the news lately. In the past week or so, major global corporations Apple, Burger King and Jeep, as well as customer service technology vendor Zendesk, have all been hacked -- to say nothing of apparent intrusions into systems governing the country’s infrastructure by the Chinese military.

Let’s take a look at exactly what has been happening in the world of high-profile hacking in recent days, starting with Apple.

**Apple - Lights Out for Java?**

Apple employees visiting a site for iPhone developers that was apparently infected with [Java-based malware](https://blogs.computerworld.com/mac-os-x/21808/apple-closes-java-hack-and-why-its-time-switch-java) that also caused a cybersecurity breach at Facebook in January had their corporate Macs hacked. As reported by Computerworld, [Apple](https://www.cmswire.com/news/topic/apple) resolved the situation by issuing a Java for OS X 2013-001 1.0 update.

However, Computerworld says many experts are urging users of any platform (and this specific malware reportedly targeted Macs) to simply “shut off Java.” Java is said to pose unique risks as a cross-platform application and Cisco has estimated 80 percent of cyberattacks exploit Java vulnerabilities, with online ads being a major culprit. Apple’s latest Java update actually disables the Java SE 6 applet plug-in, which Computerworld says is tantamount to Apple abandoning Java.

**Burger King, Jeep Discover the Dark Side of Social**

While brands are exhorted to “be social” and maintain an active presence on leading consumer social networks such as Twitter, this week Burger King there is a [dark side to social branding](http://econsultancy.com/ca/blog/62167-dealing-with-a-twitter-hack-lessons-from-burgerking?utm_medium=email&utm_source=daily_pulse).

An Econsultancy blog post reports that hackers who were possibly (but as of yet not publicly confirmed to be) affiliated with the global hacker organization Anonymous broke into Burger King’s Twitter account, changed the name and image to that of chief Burger King rival McDonald’s, and spent an hour sending out images and comments hurtful to the fast food chain’s brand.

Econsultancy essentially gives Burger King a pass as far as allowing this to actually occur, since groups such as Anonymous are capable of defeating the cyber [security](https://www.cmswire.com/news/topic/security) efforts of world governments, but rebukes the company for only sending out a single tweet obliquely referring to an “interesting day” once the hack was fixed and planning to apologize publicly on Facebook, rather than Twitter.

The post also advises Twitter to take additional steps, such as two-step authentication, to protect corporate clients and reminds companies to use basic anti-hacking precautions such as constantly monitoring [social media](https://www.cmswire.com/news/topic/social+media) accounts, using passwords that cannot easily be guessed, avoiding third-party apps and limiting authorized access.

Jeep was victimized by a similar [Twitter hack](https://www.cnbc.com/id/100471409) a couple of days before the Burger King hack, with its page switched to promote Cadillac and a series of tweets confessing to purported drug use by Jeep executives and containing racial epithets being sent out. CNBC reports that Cadillac quickly denied any involvement and Jeep quickly regained control of the account.

Speculation for this hack has also focused on Anonymous as well as the hack group LulzSec, but Gizmodo reports that a New England DJ with a [juvenile history of sophisticated hacking](https://gizmodo.com/5985353/exclusive-the-burger-king-and-jeep-hacker-is-probably-this-dj-from-new-england) may actually be to blame.

**Zendesk Support Info Hacked**

In a less high-profile but still significant case, customer support technology vendor Zendesk publicly announced on its site yesterday that earlier this week, a [hacker gained access to its system](https://www.zendesk.com/blog/weve-been-hacked) and downloaded support information of three customers.

Zendesk has since patched the vulnerability and ended the hacker’s access, but the company believes customer email addresses and support email subject lines were stolen and is helping the customers respond. This attack is a reminder that hackers do not limit themselves to major public attacks on multibillion dollar global enterprises.

**A New Form of Warfare?**

More troubling than any individual hacking attempt, even by organized crime or hacker groups, is the rising threat of unfriendly governments using hacking as a means of espionage or even warfare.

Reporting on a recent highly publicized study from computer security firm Mandiant, the New York Times says a [secretive group within the People’s Liberation Army of China has been engaging in widespread hacking](https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all&_r=0) of “companies involved in the critical infrastructure of the United States -- its electrical power grid, gas lines and waterworks.”

The Chinese Army has also reportedly hacked into the systems of defense contractors, US government agencies and major corporations such as Coca-Cola (there is also speculation the Chinese military was tied to the Apple attack, although Apple has not publicly commented).

As devastating as personal data/identity theft, brand damage and other consequences of corporate hacking can be, these results pale in comparison with the troubling consequences of a totalitarian nation potentially gaining the ability to shut down the US power grid or seriously disrupt the oil supply. The world is online and there is no feasible way to bring it back offline, but the people responsible for maintaining online security need to realize there is more at stake than a restaurant chain suffering some short-term embarrassment.

Reference <https://www.computer.org/publications/tech-news/trends/5-cybersecurity-threats-to-be-aware-of-in-2020/>

5 Cybersecurity Threats to Be Aware of in 2020

By Gaurav Belani

[Visit our Jobs Board](https://jobs.computer.org/jobseekers/index.cfm)



*Source:*[*https://www.needpix.com/photo/download/942931/ransomware-cyber-crime-malware-encryption-malicious-ransom-privacy-hack-hacker*](https://www.needpix.com/photo/download/942931/ransomware-cyber-crime-malware-encryption-malicious-ransom-privacy-hack-hacker)

The risk and severity of cyber-attacks have clearly grown over the past few years. In fact, since the year 2018, mankind has witnessed the most horrific cases of cybercrimes related to [massive data breaches](https://www.forbes.com/sites/kateoflahertyuk/2019/03/11/marriott-ceo-reveals-new-details-about-mega-breach/#340b9f74155c), [flaws in microchips](https://www.technologyreview.com/f/611879/intels-foreshadow-flaws-are-the-latest-sign-of-the-chipocalypse/), [cryptojacking](https://medium.com/altcoin-magazine/cryptojacking-is-getting-out-of-control-4-famous-cases-3687bd0f00a0), and many others.

It goes without saying that the advancement of technology and the wide use of digital media is making attackers smarter by the day. Further, these cybercriminals take advantage of individuals and firms who pay less heed to cybersecurity. They target everything from a [newly-launched blog](https://websitesetup.org/how-to-start-a-blog-guide/) to an established online store to gain access to sensitive information.

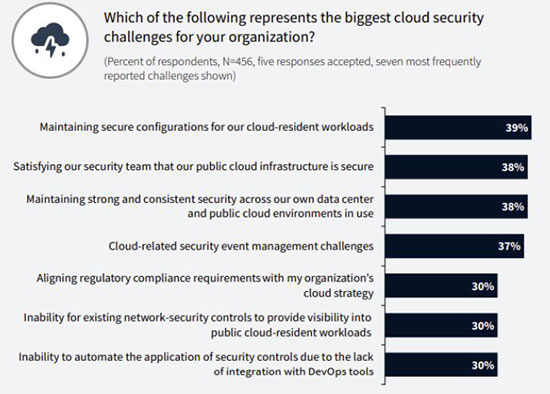
Every other day we read news related to cybersecurity threats like ransomware, phishing, or IoT-based attacks. However, 2020 comes with a whole new level of cybersecurity threats that businesses need to be aware of. In fact, a [report by Threat Horizon](https://www.securityforum.org/research/threat-horizon-2019/) reveals that in the coming years, organizations will face cyber threats under three key themes –

* **Disruption:** Over-dependence on fragile connectivity will increase the risk of premeditated internet outages that compromise business operations. Cybercriminals will use ransomware to hijack the Internet of Things.
* **Distortion:** Spread of misinformation by bots and automated sources will cause compromise of trust in the integrity of information.
* **Deterioration:** Rapid advances in smart technologies and conflicting demands posed by evolving national security will negatively impact an enterprise’s ability to control information.

Cybersecurity is all about staying ahead of threats rather than managing them later. Read on to know and prepare for the top cybersecurity threats that organizations will face in 2020.

1. **Cloud Vulnerability**
2. The [Oracle and KPMG Cloud Threat Report 2019](https://www.oracle.com/cloud/cloud-threat-report/) reveals that cloud vulnerability is and will continue to be one of the biggest cybersecurity challenges faced by organizations. This is because enterprises are leveraging cloud applications and storing sensitive data related to their employees and business operations on the cloud.

The adoption of the cloud is creating new challenges for firms and exacerbating the old ones.



*Source:*[*https://www.oracle.com/a/ocom/docs/dc/final-oracle-and-kpmg-cloud-threat-report-2019.pdf?elqTrackId=063c9f4a2a5b465ab55b734007a900f0&elqaid=79797&elqat=2*](https://www.oracle.com/a/ocom/docs/dc/final-oracle-and-kpmg-cloud-threat-report-2019.pdf?elqTrackId=063c9f4a2a5b465ab55b734007a900f0&elqaid=79797&elqat=2)

[Forbes](https://www.forbes.com/sites/louiscolumbus/2018/01/07/83-of-enterprise-workloads-will-be-in-the-cloud-by-2020/#2e4685776261) predicts that 83 percent of enterprise workload will be on the cloud by 2020. These organizations make tempting targets for malicious hackers. Data breach, misconfiguration, insecure interfaces and APIs, account hijacking, malicious insider threats, and DDoS attacks are among the top cloud security threats that will continue to haunt firms failing to invest in a robust cloud security strategy.

Finally, cloud companies like Google and Amazon storing other companies’ data are heavily investing in improving their cloud security. However, that doesn’t make them immune to deep cyber intrusions like the [Operation Cloud Hopper](https://www.bankinfosecurity.com/cloud-hopper-major-cloud-services-victims-named-a-12695).

1. **AI-Enhanced Cyberthreats**
2. AI and machine learning have disrupted every industry. Owing to its ability to create a significant impact on marketing services, manufacturing, security, supply chain management, and other fields, AI is finding its way into the business mainstream.

However, AI is proving to be a boon for cybercriminals too. Think about it – the AI capabilities used to identify and stop cyberattacks can also be used by hackers to launch sophisticated cyberattacks in the form of complex and [adaptive malicious software](https://www.techrepublic.com/article/how-ai-enhanced-malware-poses-a-threat-to-your-organization/).

In fact, AI fuzzing (AIF) and machine learning (ML) poisoning are all set to be the next big cybersecurity threats.

1. **AI Fuzzing**
2. AI fuzzing integrates AI with [traditional fuzzing techniques](https://cybersecurity.springeropen.com/articles/10.1186/s42400-018-0002-y) to create a tool that detects system vulnerabilities. This can be a boon or a bane. Though AI fuzzing can help enterprises detect and fix the exploitable vulnerabilities in their system, it can also be used by cybercriminals to start, automate, and accelerate [zero-day attacks.](https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html)
3. **Machine Learning Poisoning**
4. If a hacker targets a machine learning model and injects instructions into it, the system becomes vulnerable to attacks. Machine learning models typically use data that is crowd-sourced or taken from social media. They also exploit user-generated information such as satisfaction ratings, purchasing histories, or web traffic. Cybercriminals engaging in MI poisoning could potentially use malicious samples or introduce backdoors or Trojans to poison training sets and compromise the system.

1. **Smart Contract Hacking**
2. Though smart contracts are in their early stages of development, businesses are using them to execute some form of digital asset exchange or the other. In fact, it’s smart contracts that make [Ethereum](https://www.newsbtc.com/2019/11/19/how-ethereum-is-shaping-up-to-be-a-digital-finance-powerhouse/) famous.

Smart contracts are software programs that carry self-executing code. This code enables developers to create the rules and processes that build a blockchain-based application. Consequently, these contracts are a prime target of online criminals looking to compromise such applications. Moreover, since it’s a brand new field, technologists are just about getting to know how to design them and security [researchers are still finding bugs](https://www.technologyreview.com/s/610392/ethereums-smart-contracts-are-full-of-holes/) in some of them. These vulnerabilities make it easy for criminals to hack the contracts.

As this technology continues to mature, smart contract hacking will pose a significant threat to businesses in 2020 and beyond.

1. **Social Engineering Attacks**
2. Social engineering attacks like phishing have always been used by attackers to trick victims into surrendering sensitive information like login details and credit card information. Though most organizations are enhancing their email security to block phishing attacks, cybercriminals are coming up with [sophisticated phishing kits](https://www.helpnetsecurity.com/2018/02/08/credential-phishing-kits/) that aid in data breaches and financial fraud.

Since phishing is an effective, high-reward, and minimal-investment strategy for cybercriminals to gain legitimate access to credentials, it will continue to be a big cybersecurity threat in 2020. In fact, [the 2019 Data Breach Investigations Report](https://enterprise.verizon.com/en-gb/resources/reports/dbir/) by Verizon reveals that phishing remains the number one cause of data breaches globally.

SMiShing (SMS phishing) is another form of social engineering attack that will gain prominence in the near future. The immense popularity of apps like WhatsApp, Slack, Skype, WeChat, and Signal among others is encouraging attackers to switch to these messaging platforms to trick users into downloading malware on their phones. According to Experian’s [2020 Data Breach Industry Forecast](https://www.experian.com/data-breach/data-breach-industry-forecast), SMiShing attempts from hackers will target consumers through fraudulent messages disguised as fundraising initiatives.

1. **Deepfake**
2. First [coined by Reddit users](https://towardsdatascience.com/deepfakes-an-unknown-and-uncharted-legal-landscape-faec3b092eaf) in 2017, ‘deepfake’ is a fake video or audio recording that cybercriminals use for illicit purposes. For instance, amateurs and criminals have created deepfakes by swapping people’s faces in videos or altering its audio track.

Check out this [deepfake video of Obama](https://www.youtube.com/watch?v=cQ54GDm1eL0) that uses AI to deliver fake news.

[](https://www.youtube.com/watch?v=cQ54GDm1eL0)

Embed Video – <https://www.youtube.com/watch?v=cQ54GDm1eL0>

This AI-based technology has made steady progress as algorithms are better able to process data today. As the technology matures, cybercriminals use it to foster disruption across various industry segments, mainly financial markets, media and entertainment, and politics. In fact, deepfake can pose a huge threat to the [upcoming 2020 elections](https://www.cnbc.com/2019/10/15/deepfakes-could-be-problem-for-the-2020-election.html).

In the business world, these AI-generated fake videos or audios can be used to impersonate CEOs, steal millions from enterprises, spread wrong information about them, and interrupt business operations. In the coming years, deepfake will evolve into a sophisticated and convincing method of forgery, making it a huge cybersecurity threat that organizations need to be wary of.

**Quick Tips to Brace Yourself Against Cyberthreats**

1. Prioritize cybersecurity by setting up a [security strategy](https://securityboulevard.com/2019/11/building-your-cyber-security-strategy-a-step-by-step-guide/) to assess and classify the data you handle and the type of security you need to protect them. Run a security audit on a regular basis.
2. Focus on [cybersecurity awareness](https://www.computer.org/publications/tech-news/events/cybersecurity-month-2019-tips-resources-ideas). Educate your employees on the importance of data protection and security protocols.
3. Create a unique and strong password combination and complement it with two-factor authentication to access the system.
4. Invest in cybersecurity tools like antivirus software, firewall, and other privacy tools to automatically scan threats. Install and update your antivirus software.
5. Have a strong backup policy. It will protect you from ransomware attacks.
6. Apply end-to-end encryption to all your confidential files.
7. Hack yourself! This will help you identify the vulnerabilities in the system.

**Summing Up**

In this age of digital transformation and globalization, cybercriminals are constantly looking for fresh exploits and coming up with advanced strategies to defraud and damage institutions and organizations. In light of this fact, businesses should be mindful of not just the ever-growing number of vulnerabilities but also of the cybersecurity threats that are in store.

The information shared in this post will enlighten you of the upcoming threats in 2020 so that you can proactive measures to reduce their risk.

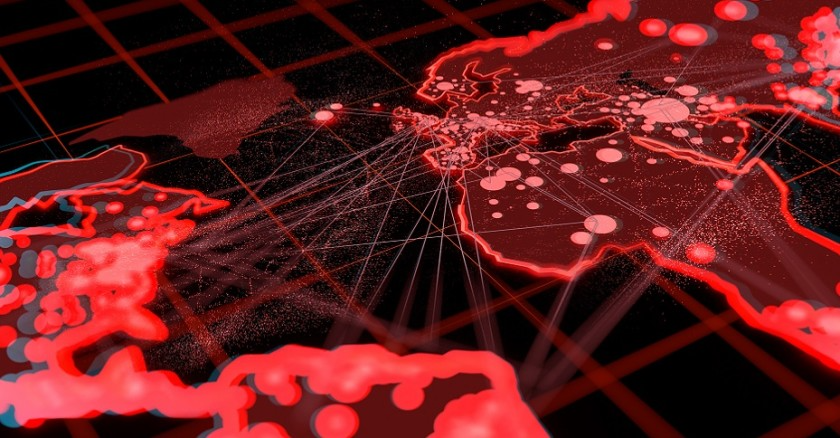
***About The Author:***  
[*Gaurav Belani*](https://in.linkedin.com/in/belanigaurav)*is a senior SEO and content marketing analyst at*[*Growfusely*](https://growfusely.com/)*, a content marketing agency that specializes in data-driven SEO. He has more than seven years of experience in digital marketing and loves to read and write about education technology, AI, machine learning, data science, and other emerging technologies. In his spare time, he enjoys watching movies and listening to music. Connect with him on Twitter at*[*@belanigaurav*](https://twitter.com/belanigaurav)*.*

*Reference*[*https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html*](https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2020-the-year-the-covid-19-crisis-brought-a-cyber-pandemic.html)

**2020: The Year the COVID-19 Crisis Brought a Cyber Pandemic**

**2020 will be remembered as a uniquely disruptive year — but not just for a global health crisis. Online life was digitally transformed, as exponential change accelerated at home and work via cyberspace.**

December 11, 2020 • Daniel Lohrmann, [Dan Lohrmann](https://www.govtech.com/authors/dan-lohrmann.html)

Ask almost anyone what the top global story was for 2020, and they will likely start with the COVID-19 pandemic. But there is much more to this story.    
  
2020 will also be remembered as the year that security events exploded and cyberincidents transformed society in numerous ways. Consider this small sample of headline stories:

* ***Bizjournals.com***: "[Cyberattacks on the rise during the Covid-19 pandemic](https://www.bizjournals.com/cincinnati/news/2020/06/01/cyberattacks-on-the-rise-during-covid-19.html)"
* ***Government Technology***: "[How Is Covid-19 Creating Data Breaches?](https://www.govtech.com/blogs/lohrmann-on-cybersecurity/how-is-covid-19-creating-data-breaches.html)"
* ***BBC*:** "[Coronavirus: How the world of work may change forever](https://www.bbc.com/worklife/article/20201023-coronavirus-how-will-the-pandemic-change-the-way-we-work)"
* ***Interpol.int***: "[INTERPOL report shows alarming rate of cyberattacks during COVID-19](https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19)"
* ***Techxplore.com***: "[Ransomware surge imperils hospitals as pandemic intensifies](https://techxplore.com/news/2020-11-ransomware-surge-imperils-hospitals-pandemic.html)"
* ***PR Newswire***: "[Top Cyber Security Experts Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic](https://www.prnewswire.com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html)"
* ***ZDNe*t:** "[COVID-19 pandemic delivers extraordinary array of cybersecurity challenges](https://www.zdnet.com/article/roundup-the-coronavirus-pandemic-delivers-an-array-of-cyber-security-challenges/)"
* ***Maritime Executive*:** "[Maritime Cyberattacks Up by 400 Percent](https://www.maritime-executive.com/article/report-maritime-cyberattacks-up-by-400-percent)"

The magnitude (breadth, depth and height) of this overall online set of Internet trends has revealed many positive benefits. For example, numerous people are enjoying the quality of life benefits received in the move to [working from home](https://www.govtech.com/blogs/lohrmann-on-cybersecurity/office-work-will-we-ever-go-back.html).  
  
Going further, some experts argue that technology has been a silver lining during this pandemic, since so many communication, business and personal interactions moved online without significant outages or business impacts for 80 percent of the economy (excluding travel, hotels, restaurants, etc.). In a sense, cyberspace has stepped up to the challenges brought by COVID-19 in ways that did not (and could not) happen during the last major pandemic in 1918.  
  
But the negative cybersecurity impacts of these online changes have led many experts to summarize the combined events this year as a growing “cyber pandemic.” In this year-end perspective, global people, process and technology changes in moving to digital transactions from home have been a type of “Trojan horse” for cybercriminals and nation state bad actors.  
  
I jumped on this bandwagon as an early voice using this new term. For example, in early June I asked: “[Is a Cyber Pandemic Coming](https://www.govtech.com/blogs/lohrmann-on-cybersecurity/is-a-cyber-pandemic-coming.html)?” This was right after the CEO of Checkpoint told a four-day online summit organized by the Israeli-American Council and the Peres Center for Peace and Innovation that “[we need to prepare for the coming cyber pandemic](https://www.jpost.com/jpost-tech/check-point-ceo-we-need-to-prepare-for-the-coming-cyber-pandemic-629933).”    
  
Going further, consider these global stories:

* ***Tripwire***: "[The COVID-19 Pandemic Dominates the Cybersecurity World](https://www.tripwire.com/state-of-security/featured/covid-19-pandemic-dominates-cybersecurity-world/)"
* ***MetaCompliance***: "[The Next Global Crisis: A Cyber Security Pandemic](https://www.metacompliance.com/blog/the-next-global-crisis-a-cyber-security-pandemic/)"
* ***Forbes*:**"[Cyber Pandemic Survival Guide: Three Things For Future Consideration](https://www.forbes.com/sites/forbestechcouncil/2020/08/18/cyber-pandemic-survival-guide-three-things-for-future-consideration/?sh=417b43792442)"
* ***Finfeed*:** "[Australia under cyberattack: is the world facing a cyber pandemic?](https://finfeed.com/features/australia-under-cyberattack-world-facing-cyber-pandemic/)"
* ***CNBC***: "[Middle East facing ‘cyber pandemic’ as Covid exposes security vulnerabilities, cyber chief says](https://www.cnbc.com/2020/12/06/middle-east-facing-cyber-pandemic-amid-covid-19-uae-official-says.html)"

Here is an excerpt from the last *CNBC* article: "The UAE has seen an 'at least 250% increase' in cyberattacks this year, Al Kuwaiti said, as the pandemic forced organizations around the world to reconsider how and where they work and hackers and malicious actors took advantage of increased digital adoption.  
  
"'There is a cyber pandemic, not only a biological pandemic,' he said.  
  
"Al Kuwaiti also said that the United Arab Emirates was the target of 'huge attacks' from 'activists' against the UAE after it established formal ties with Israel in August."  
  
**What Are the Results of a Cyber Pandemic?**  
  
Defining a cyber pandemic is a bit like defining a “perfect storm” — only this storm is in cyberspace. There are many moving parts, which include an “all of the above” list of threats and cyberattacks listed in items No. 2-5 below. From ransomware to data breaches and from election security to unemployment fraud, COVID-19 has in many ways unleashed a new set of challenges and/or accelerated existing challenges within global enterprises.  
  
What is clear is that technology and security pros struggled in 2020 to respond as quickly to the changing environment as did the bad actors, who took advantage of unprecedented shifts in people, processes and technology within governments and worldwide companies.        
  
One specific example comes from the World Health Organization (WHO), which [reported a fivefold increase in cyberattacks](https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance) in late April 2020. Here’s an excerpt:  
  
"Since the start of the COVID-19 pandemic, WHO has seen a dramatic increase in the number of cyber attacks directed at its staff, and email scams targeting the public at large.  
  
"This week, some 450 active WHO email addresses and passwords were leaked online along with thousands belonging to others working on the novel coronavirus response.  
  
"The leaked credentials did not put WHO systems at risk because the data was not recent. However, the attack did impact an older extranet system, used by current and retired staff as well as partners.  
  
"WHO is now migrating affected systems to a more secure authentication system."  
  
Meanwhile, *Wired* magazine offered another trend during the pandemic, namely that "[Internet Freedom Has Taken a Hit During the COVID-19 Pandemic](https://www.wired.com/story/internet-freedom-covid-19-2020/)." Here’s an excerpt from the piece: *“*From surveillance to arrests, governments are using the novel coronavirus as cover for a crackdown on digital liberty.  
  
"Almost 40 million people around the world have contracted [COVID-19](https://www.wired.com/tag/covid-19), and more than 1 million have died from the virus. The devastation has rippled even further, thanks to a global recession and rising political unrest. And as all of this unfolds, new research indicates that the governments around the world have exploited the pandemic to expand their domestic surveillance capabilities and curtail internet freedom and speech.  
  
"The human and digital rights watchdog Freedom House today published its annual [Freedom on the Net report](https://freedomhouse.org/report/freedom-net/2020/pandemics-digital-shadow), which tracks the ebb and flow of censorship laws, net neutrality protections, internet shutdowns, and more around the world. This year's report, which covers the period from June 2019 through May 2020, encompasses not only the Covid-19 pandemic but also the trade war between the US and China, which has resulted in a dramatic acceleration of the cyber sovereignty movement. Combined with numerous other geopolitical clashes that have impacted digital rights, global internet freedom has been broadly curtailed in 2020."  
  
One expert put it this way: "We’re sleepwalking into a world where our most sensitive personal and biometric data will soon be at the mercy of private companies, security agencies, and even cybercriminals."  
  
**Changing Cyber Ahead?**  
  
We will cover 2021 security industry predictions next week, but a quick mention that McKinsey believes that cybersecurity technology and service providers are [shifting priorities](https://www.mckinsey.com/business-functions/risk/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets) to support current needs: business continuity, remote work, and planning for transition to the next normal, after the pandemic:  
  
"Few corporate functions shifted priorities so much and so quickly when the COVID-19 crisis struck as corporate cybersecurity operations and the technology providers that support them did. As legions of employees suddenly found themselves in a work-from-home model, chief information-security officers (CISOs) adjusted, pivoting from working on routine tasks and toward long-term goals to establishing secure connections for newly minted remote workforces. CISOs also took steps to prevent new network threats that target remote workers and to bolster business-facing operations and e-commerce after a surge in online shopping during pandemic lockdowns.  
  
"The response to the crisis continues to press department budgets and limit resources for other, less essential functions—a situation that we believe will direct spending in fiscal year 2021, which many departments are beginning to plan for. According to new McKinsey research, overall spending should taper off from the sector’s recent rapid growth in industries that were hit hard by the COVID-19 crisis while holding steady in industries that have not been as affected.  
  
"The challenges that cybersecurity organizations face have spilled over to technology providers. Those companies have done their own pivots to keep up with customers’ shifting needs and to institute new ways of doing business. To succeed in the post-COVID-19 era, technology providers must rethink their strategies and offerings to accommodate a new security landscape. And they must continue to monitor customers’ needs and adjust sales, service, and training accordingly."  
  
**Other Top Cyberissues In 2020**  
  
**2) Election Security:**Unlike the topic of a cyber pandemic and issues associated with COVID-19, [almost everyone predicted](https://www.govtech.com/blogs/lohrmann-on-cybersecurity/the-top-20-security-predictions-for-2020.html) a ton of attention on the U.S. presidential elections in 2020, and the experts were correct on this one.  
  
There are thousands of stories on "[How election security has become a top issue](https://www.govtech.com/blogs/lohrmann-on-cybersecurity/how-election-security-has-become-a-top-issue.html)," and there are numerous perspectives and related content that vary from [CISA Director Chris Krebs getting fired](https://www.govtech.com/people/Trump-Fires-CISA-Director-Chris-Krebs-Over-Election-Dispute.html) to [foreign influence (or not) in elections](https://www.bbc.com/news/election-us-2020-53702872) to [new rules on voting because of COVID-19](https://abcnews.go.com/Politics/states-changed-rules-voting-amid-coronavirus-pandemic/story?id=72309089).        
  
At the time of this publication, President Trump has not conceded the election, and there are still claims of fraud and more. One thing is certain, we will be talking about election security and more changes throughout the next decade.  
  
**3) More** **Ransomware** **Emergencies:** The top cyber story from 2019 was [how ransomware targeted state and local governments](https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2019-the-year-ransomware-targeted-state--local-governments.html).  
  
In 2020, the surge in ransomware attacks continued with [hospitals](https://fortune.com/2020/12/09/covid-hospitals-hackers-ransomware/), [schools](https://www.baltimoresun.com/education/bs-pr-md-baltimore-county-ransomware-20201203-20201204-5g3he4yi2je6npug3vcf7zih3i-story.html) and more being hit hard — [with bigger ransoms being paid](https://www.theverge.com/2020/8/4/21353842/garmin-ransomware-attack-wearables-wastedlocker-evil-corp).  
  
The ransomware surge trends do not bode well for organizations in 2021 and beyond, with soaring costs and [more bold plans](https://www.zdnet.com/article/ransomware-gangs-are-getting-faster-at-encrypting-networks-that-will-make-them-harder-to-stop/) from the bad actors. [Read or listen to this interview](https://legaltalknetwork.com/podcasts/digital-detectives/2020/11/ransomware-surges-what-law-firms-need-to-know/) to see why.    
  
**4) Data Breaches:**The [dramatic breach announced by U.S. cyberfirm FireEye this week](https://www.wsj.com/articles/u-s-cyber-firm-fireeye-says-it-was-breached-by-nation-state-hackers-11607461408) by nation state hackers has capped another headline-grabbing year of significant cybersecurity incidents. The *Wall Street Journal* reported that “the cybersecurity company said the attack compromised its software tools used to test the defenses of its thousands of customers.”  
  
As in previous years, significant data breaches continued, almost nonstop, throughout the year. For example, another data breach announced this week came when criminals accessed vaccine documents in a [cyberattack on the European Medicines Agency (EMA).](https://lnkd.in/eH7k2bJ) Papers relating to the Pfizer/BioNTech vaccine were reportedly targeted in the cyberattack. Similar cyberattacks leading to data breaches occurred throughout the year, but these received less attention due to the pandemic and other headline news, such as election security.  
  
The final numbers are not in yet for 2020, but the number of data records exposed has risen again. [According to Risk Based Security](https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Q3%20Data%20Breach%20QuickView%20Report.pdf):

* There were 2,953 publicly reported breaches in the first three quarters of 2020, a 51% decrease compared to the same time period last year.
* 2020 was already the “worst year on record” by the end of Q2 in terms of the total number of records exposed. The three months of Q3 added an additional 8.3 billion records to the count, bringing the number of records exposed through the end of September to a staggering 36 billion.
* Two breaches in Q3 exposed over 1 billion records each and four breaches exposed over 100 million records. Together these six breaches accounted for approximately 8 billion exposed records, or 22.3% of the records exposed through the end of Q3.
* Malicious actors continue to be the driving force behind the number of breaches occurring, while misconfigured databases and services remain the leading cause behind the number of records exposed.
* In the first three quarter of 2020, 21% of reported breaches involved the use of ransomware. These ransomware-related events contributed to the unusually high number of unknown (11.2%) and miscellaneous (10.4%) data types exposed.
* Following well established trends, the Healthcare sector had the most reported breaches, accounting for 11.5% of the events that could be attributed to a specific economic sector.

**5) Dominance of Cloud Computing Grows in Global Enterprises, With Huge Security Implications:**Another accelerating trend during the pandemic was [the growth of public- and private-sector organizations moving to cloud computing](https://blog.allstream.com/pandemic-accelerates-move-to-cloud/). These moves included everything from infrastructure to applications to full outsourcing using cloud providers ranging from Google to Amazon to Microsoft and even many smaller cloud providers.  
  
Why is this item on a 2020 cyber roundup? As *SC Magazine* points out in this piece, "[As companies scramble to the cloud, security takes center stage](https://www.scmagazine.com/home/editorial/as-companies-scramble-to-the-cloud-security-takes-center-stage/)."  
  
"Cloud security may seem a well-worn topic. But as the technology and the use cases evolve, so do the considerations for securing networks and data. We transitioned as a community from skeptical, figuring that no virtual environment could be as secure as one confined to the four walls of a data center, to apprehensive – dipping in our toes with lower risk workloads like storage and email. And now most every business, from small to large, relies at least in part on cloud to support the IT infrastructure.    
  
"But interestingly, the very tactics that contribute to both agility and security within the cloud – hybrid and multi-cloud models – can introduce vulnerabilities if not properly locked down."  
  
Much more on this topic coming in 2021, but I was surprised in 2020 that so many organizations have now created dedicated cloud security teams. Even as email, storage, data, applications, backups and much more are placed in clouds, enterprise teams are focusing more on securing those investments with cloud security solutions that have move from Cloud Access Security Brokers (CASB) to Secure Access Service Edge (SASE) network architectures.  
  
**Final Thoughts**  
  
Looking back over the past few year-end cyber summaries can also teach us a wider story on the cyber industry. Consider these “Lohrmann on Cybersecurity and Infrastructure” annual security industry headlines from the past six Decembers:

* **2014:**"[The year cyber danger doubled](https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2014-The-year-cyber-danger-doubled.html)"
* **2015:**"[The year data breaches became intimate](https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2015-the-year-data-breaches-became-intimate.html)"
* **2016:**"[The year hackers stole the show with a cause](https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2016-the-year-hackers-stole-the-show-with-a-cause.html)"
* **2017:**"[The year hurricanes devastated land, data and trust](https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2017-the-year-hurricanes-devastated-land-data-and-trust.html)"
* **2018:** "[The year privacy took center stage](https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2018-the-year-privacy-took-center-stage.html)"
* **2019**: "[The year ransomware targeted state & local governments](https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2019-the-year-ransomware-targeted-state--local-governments.html)"

While there are several wider security trends one could name from this list, one unmistakable pattern is the continued merger between the physical world and our online cyber world. With the elections in 2016 and 2020, hurricanes in 2017 and now the pandemic in 2020, worldwide headline trends and major events are dramatically impacting our online worlds in disruptive, accelerating ways.  
  
What does that tell us about the future? You’ll need to wait another week to read about our cyber industry’s trends and expert forecasts in my upcoming post on "The Top 21 Security Predictions for 2021."