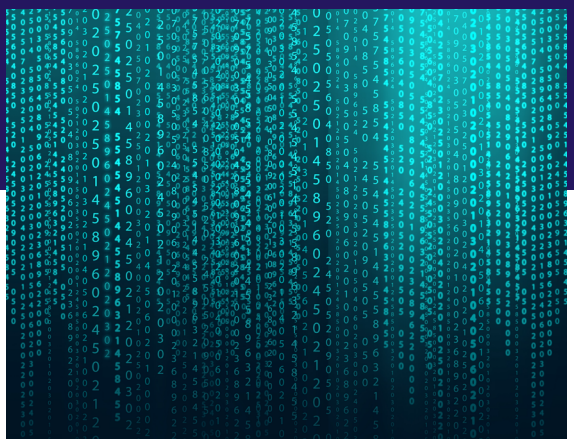
The 2020 Data Attack Surface Report



The World Will Store 200 Zettabytes of Data by 2025

Steve Morgan, Founder, Cybersecurity Ventures; Editor-in-Chief, Cybercrime Magazine
Sponsored by Arcserve

The 2020 Data Attack Surface Report predicts the total amount of data that the world will need to protect over the next 5 years.

Cybersecurity Ventures predicts that the total amount of data stored in the cloud — which includes public clouds operated by vendors and social media companies (think Apple, Facebook, Google, Microsoft, Twitter, etc.), government-owned clouds that are accessible to citizens and businesses, private clouds owned by mid-to-large-sized corporations, and cloud storage providers — will reach 100 zettabytes by 2025, or 50 percent of the world's data at that time, up from approximately 25 percent stored in the cloud in 2015.

Total global data storage is projected to exceed 200 zettabytes by 2025. This includes data stored on private and public IT infrastructures, on utility infrastructures, on private and public cloud data centers, on personal computing devices — PCs, laptops, tablets, and smartphones — and on IoT (Internet-of-Things) devices.

With this exponential data growth the opportunities — for innovation, and for cybercrime — are incalculable because data is the building block of the digitized economy.

CYBER CRIME RADIO
CYBERCRIME.RADIO

Arcserve's CTO Oussama El-Hilali

We Need to Back Up and Protect the World's Data Explosion

▸ **Listen now**

At present, approximately 5 billion people access and store data on their digital devices and the cloud. 90 percent of the human population, aged 6 years and older, or roughly 7.5 billion people, will be online and generating data by the end of this decade.

In 2020, there are 3.5 billion smartphone users worldwide, or 45 percent of the population, many of whom are "smartphone-only Internet users." The mobile app market — which serves that user base — is expected to see a rise in cloud-based apps as 5G technology proliferates and reaches 2.6 billion subscribers by 2025.

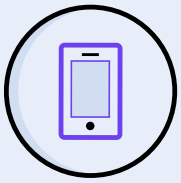
More than 2 billion people worldwide now play mobile games. The cloud gaming market, which stores its data in the cloud, is projected to skyrocket by 10X from 2017 to 2023. 5G technology will power further growth through the end of the decade.

According to one headcount projection, the world had 19 million software developers in 2019, and will reach 45 million developers by 2030, based on 20 percent year-over-year growth.

7.5 Billion

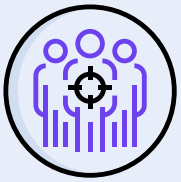
people will be online and generating data by the end of this decade

3.5 Billion



smartphone users worldwide, or 45% of the population

19 Million

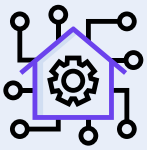


software developers in 2019 and will reach 45 million by 2030

338 Billion

lines of new software code the world will need to secure by 2025

31 Billion



connected devices in 2020 and 75 billion IoT devices by 2025

The research team at Cybersecurity Ventures predicts that the world will need to secure 338 billion lines of new software code in 2025, up from 111 billion lines of new code in 2017, based on 15 percent year-over-year growth in new code. Just Google by itself accounted for 2 billion lines of code in 2015, at which time Microsoft's Windows operating system took roughly 50 million lines of code

From connected cars to traffic lights, home security systems, connected toys and smart speakers, the combined B2C and B2B IoT market is due to reach 31 billion connected devices this year (2020) and 75 billion IoT devices by 2025, according to Cisco. Every "Thing" generates or stores data.

"Every time that we as scientists, and as human beings, try to predict data growth, it is always underestimated," says Oussama El-Hilali, chief technology officer at Arcserve. To underestimate the amount of data, which is earth's new natural resource, is to underestimate our need to protect it from cybercrime.

> *"Every time that we as scientists, and as human beings, try to predict data growth, it is always underestimated."*
>
> *- Oussama El-Hilali, CTO, Arcserve*

COVID-19

There is a massive and unexpected surge in new data being generated and stored during the novel coronavirus pandemic.
This includes biomedical literature such as PubMed, Twitter, Google Scholar, and the World Health Organization's COVID-19 database.

Apple and Google announced a partnership on COVID-19 contact tracing technology. New software from the two companies allows public health authorities globally to develop mobile apps that notify people when they may have come in contact with someone who's been diagnosed with the coronavirus.

Splunk for Good, the social impact arm of Splunk, has built an application that an individual or organization can download, populate with their own data, and use it to help get a better understanding of the data behind the pandemic.

Data related to downloads of the top 250 mobile apps worldwide jumped 52 percent in the first quarter of this year, during the early COVID-19 timeframe, according to market researcher Sensor Tower.

Data related to downloads of the top 250 mobile apps worldwide jumped 52% in the first quarter of this year

A spike in HDD (hard disk drive) demand earlier this year was the result of hyperscale data centers bulking up their storage capacity to meet the demands of remote workers due to the COVID-19 pandemic.

Prolonged COVID-19 restrictions can potentially push the share of cloud storage to the 50 percent mark a year or more earlier than predicted. Data storage and processing services from Microsoft, Google, and others that cater to remote workers are utilities much like water, electric, gas and internet access. These essential services have spiked during the first half of this year, and they may not level off for quite some time — if at all.

Dozens of vendors have responded to rising demand for consumer data storage by offering free work-from-home plans during the COVID-19 pandemic. There are also resources to help support the sudden rise of remote workers while making sure that distributed data remains protected from loss and cyberattacks.

Ransomware

Ransomware, the fastest-growing cybercrime, is the most infectious data disease known to humankind. Cybersecurity Ventures predicts that a business will be the victim of a ransomware attack every 11 seconds by 2021, up from every 14 seconds in 2019, and every 40 seconds in 2016.

When factoring in consumers, the estimated figures are closer to a ransomware attack (on a business or individual) occurring every 5 seconds by 2021.

Global ransomware damage costs are predicted to reach $20 billion by 2021 — which is 57X more than it was in 2015. "Ransomware gangs have also been changing up their tactics, attacking data backups and workloads stored in the cloud to force victims into paying ransoms," states Arcserve's El-Hilali.

A new report from Arcserve indicates that 59 percent of consumers would likely avoid doing business with an organization that had experienced a cyberattack in the past year.

Arcserve's report included a survey of nearly 2,000 consumers across North America, the United Kingdom, France, and Germany, which found that 70 percent believe businesses aren't doing enough to adequately secure their personal information and assume it has been compromised without them knowing it.

The rapid growth of internet users, the world's data explosion, and ransomware attacks on businesses and individuals, all taken together, have the potential to erode consumer trust in underprotected brands across all industries. The Arcserve study found that 25 percent of consumers will abandon a product or service in favor of a competitor after a single ransomware-related service disruption, failed transaction, or instance of inaccessible information.

59%
Of Consumers

would likely avoid doing business with an organization that had experienced a cyberattack in the past year.

70%
Of Consumers

believe businesses aren't doing enough to adequately secure their personal information

25%
Of Consumers

will abandon a product or service in favor of a competitor after a single ransomware-related service incident

Data Protection

A series of discussions between the editors at Cybersecurity Ventures and Fortune 500 CISOs (chief information security officers) surfaced five top data protection considerations (for organizations of all sizes and types) — none of which are foolproof, but all of which are critical security steps.

1. **Encryption.** Any data with the potential to cause financial or reputational harm to an organization if it were exposed or manipulated should be encrypted.

2. **Backup and Recovery.** Every company has been (or will be) hacked, and most cyber intruders go undetected for prolonged periods of time. It is therefore critical that organizations back up in ways that enable them to restore data to its unaffected pre-breach state.

3. **Consumer Transparency.** All companies should not only adhere to GDPR and other compliance standards, but they should proactively convey it to consumers. New laws have shifted control to consumers over how their data is stored and managed — and organizations should demonstrate their commitment.

4. **Cyberinsurance.** Ransomware should be covered by cyberinsurance policies — which typically reimburse for data loss damages — even if an organization is (unintentionally) negligent or imperfect in its backup practices.

5. **Hire Experts.** It is critical to have people (on staff, contractors, or through vendor relationships) contractually available, at all times, with deep domain subject matter expertise in all aspects of data security — legal, technical, operational, and disaster recovery.

> ***"Businesses must do more to ensure they're protecting their data from cybercriminals and mitigating the chance they'll experience extended downtime."***
>
> ***- Oussama El-Hilali, CTO, Arcserve***

Zettabytes

The zettabyte is a multiple of the unit byte for digital information. The prefix zetta indicates multiplication by the seventh power of 1000 or 1021 in the International System of Units (SI). A zettabyte is one sextillion (one long scale trilliard) bytes. The unit symbol is ZB.

200,000,000,000,000,000,000,000 bytes (200 ZB) of data will be stored globally by 2025.

100,000,000,000,000,000,000,000 bytes (100 ZB) of data will be stored in the cloud by 2025.

A zettabyte is equal to approximately a thousand exabytes, a billion terabytes, or a trillion gigabytes.

What's a yottabyte?

About

Cybersecurity Ventures is the world's leading researcher and publisher covering the global cyber economy, and a trusted source for cybersecurity facts, figures, predictions, and statistics.

Arcserve, sponsor of the 2020 Data Attack Surface Report, provides exceptional solutions to protect the priceless digital assets of organizations in need of full scale, comprehensive data protection.