134 Cybersecurity Statistics and Trends For

[**Sursa: Compania Varonis**, https://www.varonis.com/blog/cybersecurity-statistics/]

Recent trends, side effects of a global pandemic and cybersecurity statistics reveal a huge increase in hacked and breached data from sources that are increasingly common in the workplace, like mobile and IoT devices. On top of this, COVID-19 has ramped up remote workforces, making inroads for cyber attacks.

Additionally, recent security research suggests most companies have unprotected data and poor cybersecurity practices in place, making them vulnerable to data loss. To successfully fight against malicious intent, it's imperative that companies make cybersecurity awareness, prevention and security best practices a part of their culture.

In order to give you a better idea of the current state of overall security, we've compiled over 100 cybersecurity statistics for 2021. Hopefully, this will help show the prevalence and need for cybersecurity in all facets of business. This includes data breaches, hacking stats, different types of cybercrime, industry-specific stats, spending, costs and the cybersecurity career field.

For more in-depth security insights check out our cybersecurity whitepapers.

Overview: 2021 Cybersecurity Trends to Watch For

2020 brought with it several trials and triumphs. COVID-19 has forced companies to create remote workforces and operate off cloud-based platforms. The rollout of 5G has made connected devices, well, more connected than ever. All this to say, the cybersecurity industry has never been more important. These recent events and the below cybersecurity statistics and figures considered, here are some industry trends and also predictions to watch for in 2021 and beyond.

- Remote workers will continue to be a target for cybercriminals.
- As a side effect of remote workforces, cloud breaches will increase.
- The cybersecurity skills gap will remain an issue.
- As a result of 5G increasing the bandwidth of connected devices, IoT devices will become more vulnerable to cyber attacks.

11 Impactful Cybersecurity Facts and Stats

95% of cybersecurity breaches are caused by human error. [Cybint].

The worldwide information security market is forecast to reach $170.4 billion in 2022, according to Gartner. This is due in large part to organizations evolving their defenses against cyber threats — and a rise in such threats, including in their own companies. According to Cybint, 95% of cybersecurity breaches are caused by human error. It's a telling takeaway about the cybersecurity landscape, and we've outlined more to give an idea of the field as a whole, along with the overall impact of cyber attacks.

1. 95% of cybersecurity breaches are caused by human error. (Cybint)
2. The worldwide information security market is forecast to reach $170.4 billion in 2022. (Gartner)
3. 88% of organizations worldwide experienced spear phishing attempts in 2019. (Proofpoint)

4. 68% of business leaders feel their cybersecurity risks are increasing. (Accenture)
5. On average, only 5% of companies' folders are properly protected. (Varonis)
6. Data breaches exposed 36 billion records in the first half of 2020. (RiskBased)
7. 86% of breaches were financially motivated and 10% were motivated by espionage. (Verizon)
8. 45% of breaches featured hacking, 17% involved malware and 22% involved phishing. (Verizon)
9. Between January 1, 2005, and May 31, 2020, there have been 11,762 recorded breaches. (ID Theft Resource Center)
10. The top malicious email attachment types are .doc and .dot which make up 37%, the next highest is .exe at 19.5%. (Symantec)
11. An estimated 300 billion passwords are used by humans and machines worldwide. (Cybersecurity Media)

"It's the threats you don't see coming that get you, and this was an eye opener."

Largest Data Breaches and Hacking Statistics

The average cost of a data breach is $3,86 million as of 2020 [IBM].

The increasing amount of large-scale, well-publicized breaches suggests that not only are the number of security breaches going up — they're increasing in severity, as well. Data breaches expose sensitive information that often leaves exposed users at risk for identity theft, ruin companies' reputations and almost always leave the company liable for compliance violations.

See the data breach statistics below to help quantify the effects, motivations and causes of these damaging attacks.

Impactful Hacking Stats

12. The average cost of a data breach is $3.86 million as of 2020. (IBM)
13. The average time to identify a breach in 2020 was 207 days. (IBM)
14. And the average lifecycle of a breach was 280 days from identification to containment. (IBM)
15. Personal data was involved in 58% of breaches in 2020. (Verizon)
16. Security breaches have increased by 11% since 2018 and 67% since 2014. (Accenture)
17. 64% of Americans have never checked to see if they were affected by a data breach. (Varonis)
18. 56% of Americans don't know what steps to take in the event of a data breach. (Varonis)

Historic Data Breaches

19. In 2020, a Twitter breach targeted 130 accounts, including those of past presidents and Elon Musk, resulted in attackers swindling $121,000 in Bitcoin through nearly 300 transactions. (CNBC)
20. In 2020, Marriott disclosed a security breach impacted data of more than 5.2 million hotel guests. (Marriott)
21. The 2019 MGM data breach resulted in hackers leaking records of 142 million hotel guests. (CPO Magazine)
22. 500 million consumers, dating back to 2014, had their information compromised in the Marriott-Starwood data breach made public in 2018. (CSO Online)

23. In 2018, Under Armor reported that its “My Fitness Pal” was hacked, affecting 150 million users. (Under Armour)
24. In 2017, 147.9 million consumers were affected by the Equifax Breach. (Equifax)
25. The Equifax breach cost the company over $4 billion in total. (Time Magazine)
26. In 2017, 412 million user accounts were stolen from Friendfinder’s sites. (Wall Street Journal)
27. 100,000 groups in at least 150 countries and more than 400,000 machines were infected by the Wannacry virus in 2017, at a total cost of around $4 billion. (Technology Inquirer)
28. In 2016, Uber reported that hackers stole the information of over 57 million riders and drivers. (Uber)
29. Uber tried to pay off hackers to delete the stolen data of 57 million users and keep the breach quiet. (Bloomberg)
30. In one of the biggest breaches of all time,3 billion Yahoo accounts were hacked in 2013. (New York Times)

Cyber Crime Statistics by Attack Type

Phishing attacks account for more than 80% of reported security incidents [CSO online]

It’s crucial to have a grasp of the general landscape of metrics surrounding cybersecurity issues, including what the most common types of attacks are and where they come from. Some of these most common attacks include phishing, whaling, malware, social engineering, ransomware and Distributed Denial of Service (DDoS) attacks.

There are new malware and viruses being discovered every day.

Ransomware and Malware

31. The average ransomware payment rose 33% in 2020 over 2019, to $111,605. (Fintech News)
32. In 2018, an average of 10,573 malicious mobile apps were blocked per day. (Symantec)
33. 94% of malware is delivered by email. (CSO Online)
34. The average cost of a ransomware attack on businesses is $133,000. (SafeAtLast)
35. 48% of malicious email attachments are office files. (Symantec)
36. Ransomware detections have been more dominant in countries with higher numbers of internet-connected populations, and the U.S. ranks highest with 18.2% of all ransomware attacks. (Symantec)
37. Most malicious domains, about 60%, are associated with spam campaigns. (Cisco)
38. About 20% of malicious domains are very new and used around one week after they are registered. (Cisco)

Phishing

39. After declining in 2019, phishing increased in 2020 to account for 1 in every 4,200 emails. (Symantec)
40. 65% of groups used spear-phishing as the primary infection vector. (Symantec)
41. 1 in 13 web requests lead to malware. (Symantec)
42. Phishing attacks account for more than 80% of reported security incidents. (CSO Online)
43. $17,700 is lost every minute due to a phishing attack. (CSO Online)

IoT, DDos, and Other Attacks

44. By 2023, the total number of DDoS attacks worldwide will be 15.4 million. (Cisco)

45. Attacks on IoT devices tripled in the first half of 2019. (CSO Online)
46. Malicious PowerShell scripts blocked in 2018 on the endpoint increased 1,000%. (Symantec)
47. The Mirai-distributed DDoS worm was the third most common IoT threat in 2018. (Symantec)
48. 30% of data breaches involve internal actors. (Verizon)
49. IoT devices experience an average of 5,200 attacks per month. (Symantec)
50. 90% of remote code execution attacks are associated with cryptomining. (Purplesec)
51. 69% of organizations don't believe the threats they're seeing can be blocked by their anti-virus software.(Ponemon Institute's Cost of Data Breach Study)
52. 1 in 36 mobile devices have high- risk apps installed. (Symantec)

Cybersecurity Compliance and Governance Statistics

On average, every employee has access to 11 million files.

With new threats emerging every day, the risks of not securing files is more dangerous than ever, especially for companies and for companies with a remote workforce. More severe consequences are being enforced as stricter legislation passes in regions across the world. Some stand-outs from recent years include the European Union's 2018 General Data Protection Regulation (GDPR) and California's 2020 California Consumer Privacy Act (CCPA).

Companies need to take note of the lessons learned from the GDPR, as more iterations are expected to pass across the globe in the coming years. It's crucial to properly set permissions on files and get rid of stale data. Keeping data classification and governance up to par is instrumental to maintaining compliance with data privacy legislation like HIPAA, SOX, ISO 27001 and more.

53. 66% of companies see compliance mandates driving spending. (CSO Online)
54. In 2018, businesses spent $1.3 million on average to meet compliance requirements and were expected to put in an additional $1.8 million. (IAAP)
55. On average, every employee has access to 11 million files. (Varonis)
56. 15% of companies found 1,000,000+ files open to every employee. (Varonis)
57. 17% of all sensitive files are accessible to all employees. (Varonis)
58. About 60% of companies have over 500 accounts with non-expiring passwords. (Varonis)
59. More than 77% of organizations do not have an incident response plan. (Cybint)

GDPR Cybersecurity Statistics

60. Companies reportedly spent $9 billion on preparing for the GDPR and, in 2018, legal advice and teams cost UK FTSE 350 companies about 40% of their GDPR budget or $2.4 million. (Forbes)
61. 88% of companies spent more than $1 million on preparing for the GDPR. (IT Governance)
62. In the GDPR's first year, there were 144,000 complaints filed with various GDPR enforcement agencies and 89,000 data breaches recorded. (EDPB)
63. 1,000 news sources blocked EU readers to avoid the GDPR compliance rules. (Nieman Lab)
64. The GDPR fines totaled $63 million in its first year. (GDPR.eu)
65. Google was fined $57 billion for GDPR violations by CNIL, a French data protection agency. (TechCrunch)
66. Since the GDPR was enacted, 31% of consumers feel their overall experience with companies has improved. (Marketing Week)
67. By 2019, only 59% of companies believed they were GDPR compliant. (ZDNet)
68. 70% of companies agree that the systems they put in place will not scale as new GDPR regulations emerge. (DataGrail)

Industry-Specific Cyber Stats

The healthcare industry lost an estimated $25 billion to ransomware attacks in 2019 [SafeAtlost].

When it comes to cybersecurity, not all industries are created equal. Industries that store valuable information like healthcare and finance are usually bigger targets for hackers who want to steal Social Security Numbers, medical records and other personal data. But really, no one is safe because lower-risk industries are also targeted due to the perception that they'll have fewer security measures in place.

Take a free 30-minute demo and see how Varonis can help keep your organization's name out of data breach news.

Healthcare

69. WannaCry ransomware attack cost the National Health Service (NHS) over $100 million. (Datto)
70. The healthcare industry lost an estimated $25 billion to ransomware attacks in 2019. (SafeAtLast)
71. More than 93% of healthcare organizations experienced a data breach in the past three years. (Herjavec Group)

Finance

72. Financial services have 352,771 exposed sensitive files on average while healthcare, pharma and biotech have 113,491 files on average — the highest when comparing industries. (Varonis)
73. 15% of breaches involved healthcare organizations, 10% in the financial industry and 16% in the public Sector. (Verizon)
74. The banking industry incurred the most cybercrime costs in 2018 at $18.3 million (Accenture)
75. Trojan horse virus Ramnit largely affected the financial sector in 2017, accounting for 53% of attacks. (Cisco)
76. The financial services industry takes in the highest cost from cybercrime at an average of $18.3 million per company surveyed. (Accenture)
77. Nearly two-thirds of financial services companies have over 1,000 sensitive files open to every employee. (Varonis)
78. Financial and manufacturing services have the highest percent of exposed sensitive files at 21%. (Varonis)
79. On average, a financial services employee has access to nearly 11 million files the day they walk in the door. For large organizations, employees have access to 20 million files. (Varonis)
80. The average cost of a financial services data breach is $5.85 million USD. (Varonis)
81. Financial services businesses take an average of 233 days to detect and contain a data breach. (Varonis)

Government

82. The U.S. government saw 1.2 billion records breached in 2018. (Purplesec)
83. Manufacturing companies account for nearly a quarter of all ransomware attacks, followed by the professional services with 17% of attacks, and then government organizations with 13% of attacks. (Security Intelligence)

84. The U.S. government allocated an estimated $18.78 billion for cybersecurity spending in 2021. (Atlas VPN)

Enterprise

85. Smaller organizations (1–250 employees) have the highest targeted malicious email rate at 1 in 323. (Symantec)
86. Lifestyle (15%) and entertainment (7%) were the most frequently seen categories of malicious apps. (Symantec)
87. Supply chain attacks were up 78% in 2019. (Symantec)

Security Spending and Cost Stats

Worldwide cybercrime costs wil hit $6 trillion annually by 2021 [Cybersecurity Ventures]. Average expenditures on cybercrime are increasing dramatically, and costs associated with these crimes can be crippling to companies who have not made cybersecurity a part of their regular budget. Cybersecurity budgeting has been increasing steadily as more executives and decision-makers are realizing the value and importance of cybersecurity investments.

88. Security services accounted for an estimated 50% of cybersecurity budgets in 2020. (Gartner)
89. The average cost of a malware attack on a company is $2.6 million. (Accenture)
90. The healthcare industry incurs the highest average data breach costs at $7.13 million. (IBM)
91. The total cost of cybercrime for each company increased by 12% from $11.7 million in 2017 to $13.0 million in 2018. (Accenture)
92. The average annual security spending per employee increased from $2,337 in 2019 to $2,691 in 2020. (Deloitte)
93. The cost of lost business averaged $1.52 million. (IBM)
94. The average cost in time of a malware attack is 50 days. (Accenture)
95. The most expensive component of a cyber attack is information loss at $5.9 million. (Accenture)
96. The average cost per lost or stolen record per individual is $146. (IBM)
97. Data breaches cost enterprises an average of $3.92 million. (CSO Online)
98. The average total cost of a data breach in smaller companies (500 employees or less) decreased in 2020, from $2.74 million in 2019 to $2.35 million in 2020. The average total cost in very large companies (more than 25,000 employees) decreased, as well, from $5.11 million in 2019 to $4.25 million. (IBM)
99. In 2019 over 2020, Scandinavia saw the largest increase in total cost of data breaches at 12%, while South Africa saw the largest decrease at 7.4%. (IBM)
100. The United States experiences the highest data breach costs in the world, at $8.64 million on average, followed by the Middle East at $6.52 million. (IBM)
101. 50% of large enterprises (with over 10,000 employees) are spending $1 million or more annually on security, with 43% spending $250,000 to $999,999, and just 7% spending under $250,000. (Cisco)
102. In 2018, spending in the cybersecurity industry reached around $40.8 billion USD. (Statista)

Cybersecurity Cost Predictions

COVID-19 is credited for a 238% rise in cyberattacks on banks in 2020.

103. Worldwide cybercrime costs will hit $6 trillion annually by 2021. (Cybersecurity Ventures)
104. Ransomware damage costs will rise to $20 billion by 2021 and a business will fall victim to a ransomware attack every 11 seconds at that time. (Cybersecurity Ventures)
105. Damage related to cybercrime is projected to hit $10.5 trillion annually by 2025. (Cybersecurity Ventures)
106. More than 70 percent of security executives believe that their budgets for fiscal year 2021 will shrink. (Mckinsey)

COVID-19 Cybersecurity Statistics

COVID-19 has impacted every industry and corner of the globe, and cyberspace is no exception. The global pandemic has paved avenues for cybercriminals to target many new victims: the healthcare industry, the unemployed, remote workers and more. Here are a few of the most impactful cybersecurity statics related to the pandemic.
105.

107. Since the pandemic began, the FBI reported a 300% increase in reported cybercrimes. (IMC Grupo)
108. 27% of COVID-19 cyberattacks target banks or healthcare organizations and COVID-19 is credited for a 238% rise in cyberattacks on banks in 2020. (Fintech News)
109. Confirmed data breaches in the healthcare industry increased by 58% in 2020. (Verizon)
110. 33,000 unemployment applicants were exposed to a data security breach from the Pandemic Unemployment Assistance program in May. (NBC)
111. Americans lost more than $97.39 million to COVID-19 and stimulus check scams. (Atlasvpn)
112. In April 2020, Google blocked 18 million daily malware and phishing emails related to Coronavirus. (Google)
113. 52% of legal and compliance leaders are concerned about third-party cyber risks due to remote work since COVID-19. (Gartner)
114. Remote work has increased the average cost of a data breach by $137,000. (IBM)
115. 47% of employees cited distraction as the reason for falling for a phishing scam while working from home. (Tessian)
116. 81% of cybersecurity professionals have reported their job function changed during the pandemic. (ISC)
117. Half a million Zoom user accounts were compromised and sold on a dark web forum in April 2020. (CPO Magazine)
118. Cloud-based cyber attacks rose 630% between January and April 2020. (Fintech News)
119. Remote workers have caused a security breach in 20% of organizations. (Malwarebytes)

Cybersecurity Job Statistics

By 2021, there will be 4 million unfilled jobs in cybersecurity globally.

As rates of cyber attacks increase, so does demand for cybersecurity professionals and, thankfully, cybersecurity budgets continue to rise. However, the imbalance of the amount of skilled cybersecurity workers along with the high demand to fill cybersecurity positions has caused a cybersecurity skills shortage that sees no end in sight.

Interested in entering the field? Now is the time as the job field and average salary is only projected to grow. Looking for cybersecurity talent? Best of luck, it may be necessary to come up with creative cybersecurity skills shortage solutions — like outsourcing tasks, starting apprenticeships and partnerships with educational and military institutions to find fresh talent.

120. 61% of companies think their cybersecurity applicants aren't qualified. (ISSA)
121. 70% of cybersecurity professionals claim their organization is impacted by the cybersecurity skills shortage. (ESG & ISSA)
122. Since 2016, the demand for Data Protection Officers (DPOs) has skyrocketed and risen over 700%, due to the GDPR demands. (Reuters)
123. 500,000 Data Protection Officers are employed (IAAP)
124. More than two-thirds of cybersecurity professionals struggle to define their career paths. (ISSA)
125. 61% of cybersecurity professionals aren't satisfied with their current job. (ISSA)
126. There was a 350 percent growth in open cybersecurity positions from 2013 to 2021.(Cybercrime Magazine)
127. 40 percent of IT leaders say cybersecurity jobs are the most difficult to fill. (CSO Online)
128. C ybersecurity engineers are some of the highest-paid positions started at $140K annually on average. (Cybint)

Security Job Prediction Stats

129. The cybersecurity unemployment rate is 0% and is projected to remain there through 2021. (CSO Online)
130. By 2021, 100% of large companies globally will have a CISO position. (Cybersecurity Ventures)
131. By 2021, there will be 4 million unfilled cybersecurity jobs globally. (Netsparker)
132. Information Security Analysts job positions in the US are expected to grow 31% from 2019–29. (Bureau of Labor Statistics)
133. Computer Network Architect job positions in the US are expected to grow 5% from 2019–29. (Bureau of Labor Statistics)
134. Computer Programmer job positions in the US are expected to decline 9% from 2019–29. (Bureau of Labor Statistics)

Below are listed some of the most important facts and figures that shape the cybersecurity field:

1) Data breachers by the numbers:
   - Hacker attack every 39 seconds, on average 2,244times a day;
   - Data breachers exposed 36 billion records in the first half of 2020;
   - Average annual security spending is $2,691 per employee;
2) Where do cyberattacks come from?
   - 48% of malicious email attachments are office files;
   - 34% of data breaches involved internal actors;
   - 65% of groups used spear-phishing as the primary infection vector;
   - $17,700 is lost every minute due a phishing attack;
3) Who's affected?
   - Organizations with 1-250 employees have the highest malicious email rate at 1 in 323;
   - Manufacturing companies account for nearly 25% of all ransomware attacks;
   - 93% of healthcare organizations experienced a data breach in the past three years;
4) Are you at risc?
   - 17% of all senzitive files are accessible to all employees;
   - On average, every employee has access to 11 million files;
   - About 60% of companies have over 500 accounts with non-expiring passwords;
   - 77% of organizations don't have an incident responce plan;
5) What's the cost?

- The average cost of a data breach is $3,86 million;
- Remote work caused the average cost of a breach to increase by $137,000;
- The average cost per lost or stolen record is $146 per individual.

Cybersecurity Statistics FAQ

Below are some of the most frequently asked questions about cybersecurity, with answers supported by more cybersecurity statistics and facts.

Q: What Are the Types of Cyber Attacks?

A: The most common cyber attack methods include phishing/ spear-phishing, rootkit, SQL injection attacks, DDoS attacks, and malware like Trojan horse, adware and spyware.

Q: How Many Cybersecurity Attacks Are There Per Day?

A: On average, hackers attack 2,244 times a day. (University of Maryland)

Q: How Frequent Are Cyber Attacks?

A: Hackers attack every 39 seconds. (University of Maryland)

10 Cybersecurity Statistics Reports

Below are some helpful cybersecurity studies and articles to deepen your knowledge about the cybersecurity landscape, as well as a few resources.

- Accenture's 2020 State of Cyber Resilience Report
- Cisco's Cybersecurity Reports
- Cybersecurity Venture's Job Study
- IAPP-EY Annual Governance Report
- IBM's 2020 Cost of Data Breach Report
- McAfee Labs Threats Report
- Symantec Internet Security Threat Report
- RiskBased Data Breach Report
- Varonis' Data Risk Report
- Verizon's 2020 Data Breach Investigations Report

There's no question that the situation with cybercrime is dire. Luckily, by assessing your business's cybersecurity risk, making company-wide changes and improving overall security behavior, it's possible to protect your business from most data breaches.

Make sure you've done everything you can do to avoid becoming a victim to an attack. Don't become a statistic, the time to change the culture toward improved cybersecurity is now.

ROB SOBERS

Rob Sobers is a software engineer specializing in web security and is the co-author of the book Learn Ruby the Hard Way.