110 Must-Know Cybersecurity Statistics for 2020

DATA SECURITY

Inside Out Security Blog » Data Security » 110 Must-Know Cybersecurity Statistics for 2020

S ERS | UPDATED: 10/26/2020

Cybersecurity issues are becoming a day-to-day struggle for businesses. Recent trends 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.

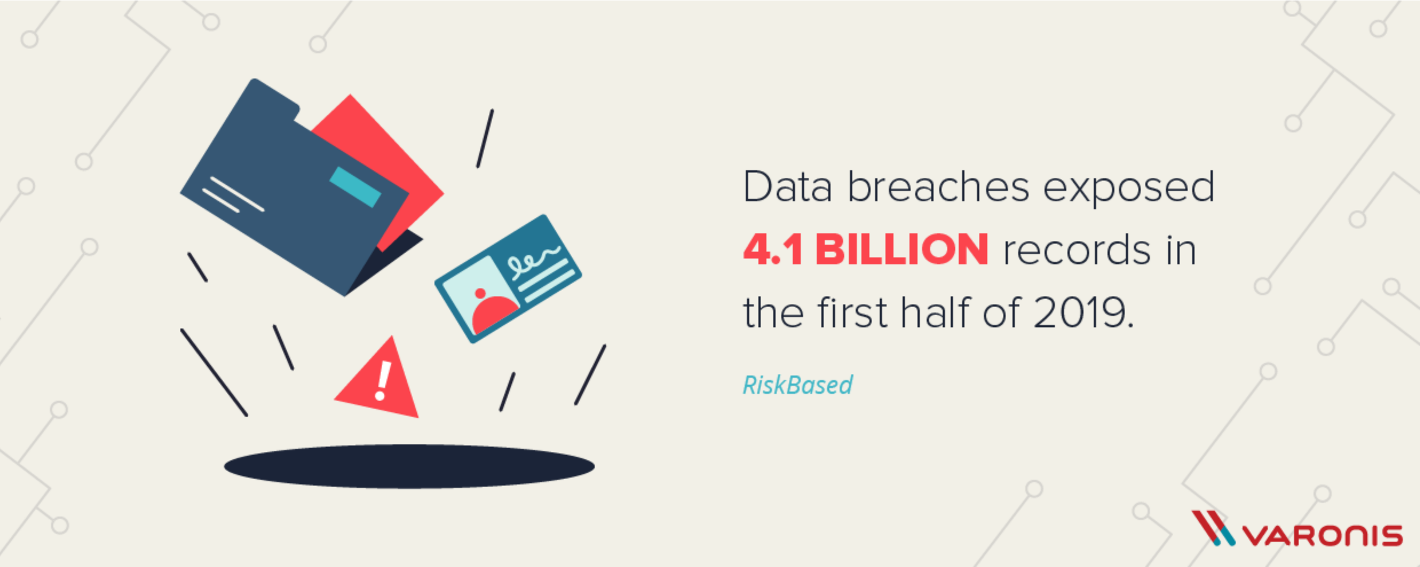
Additionally, recent security research suggests that most companies have unprotected data and poor cybersecurity practices in place, making them vulnerable to data loss. To successfully fight against malicious intent, it's imperative that companies make cybersecurity awareness, prevention and security 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 the 110 must-know cybersecurity statistics for 2020. Hopefully, this will help you paint a picture of how potentially dire leaving your company insecure can be as well as show the prevalence and need for cybersecurity in 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. Use the menu below to jump to a relevant section:

- Industry-Specific
- Spending and Costs
- Cybersecurity Jobs

11 Impactful Cybersecurity Facts and Stats



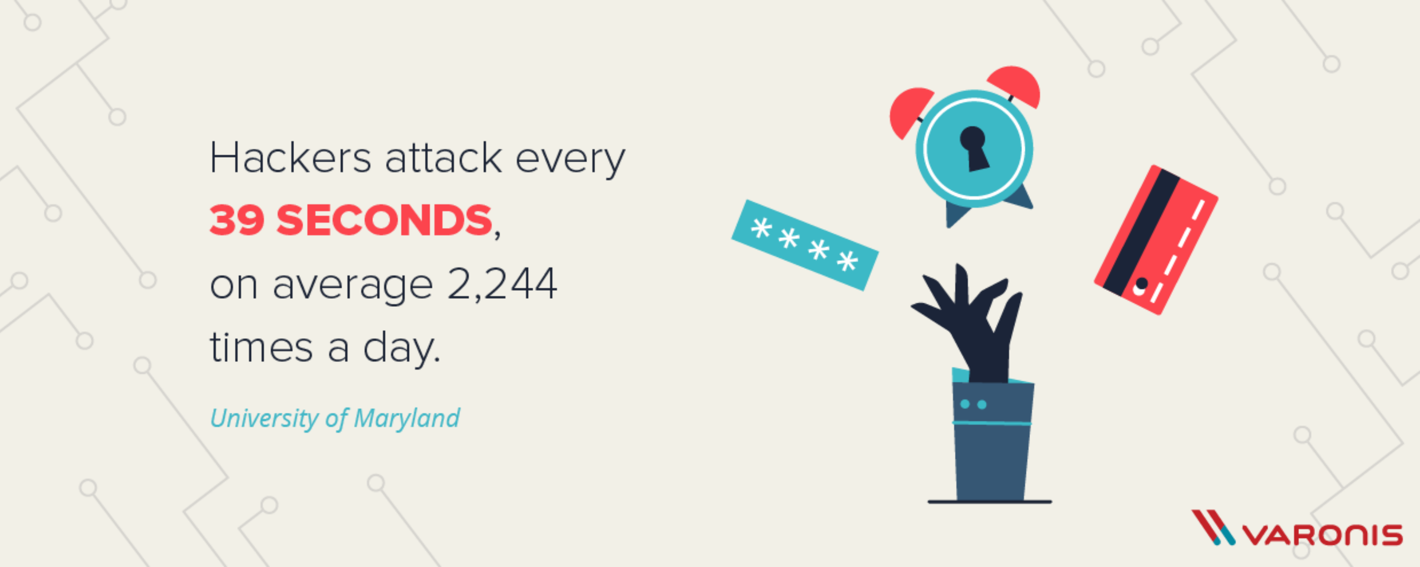
There are many important facets to cybersecurity, which are covered in greater detail below. Here we wanted to include statistics that give a good idea of the cybersecurity field as a whole, along with the overall impact of cyber attacks.

To learn more about a variety of cybersecurity topics, drop in for a free security webinar!

1. The worldwide information security market is forecast to reach $170.4 billion in 2022. (Gartner)
2. 62% of businesses experienced phishing and social engineering attacks in 2018. (Cybint Solutions)
3. 68% of business leaders feel their cybersecurity risks are increasing. (Accenture)
4. Only 5% of companies' folders are properly protected, on average. (Varonis)
5. Data breaches exposed 4.1 billion records in the first half of 2019. (RiskBased)

6. 71% of breaches were financially motivated and 25% were motivated by espionage. (Verizon)
7. 52% of breaches featured hacking, 28% involved malware and 32–33% included phishing or social engineering, respectively. (Verizon)
8. Between January 1, 2005 and April 18, 2018 there have been 8,854 recorded breaches. (ID Theft Resource Center)
9. While overall ransomware infections were down 52%, enterprise infections were up by 12% in 2018. (Symantec)
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. By 2020, the estimated number of passwords used by humans and machines worldwide will grow to 300 billion. (Cybersecurity Media)

Largest Data Breaches and Hacking Statistics



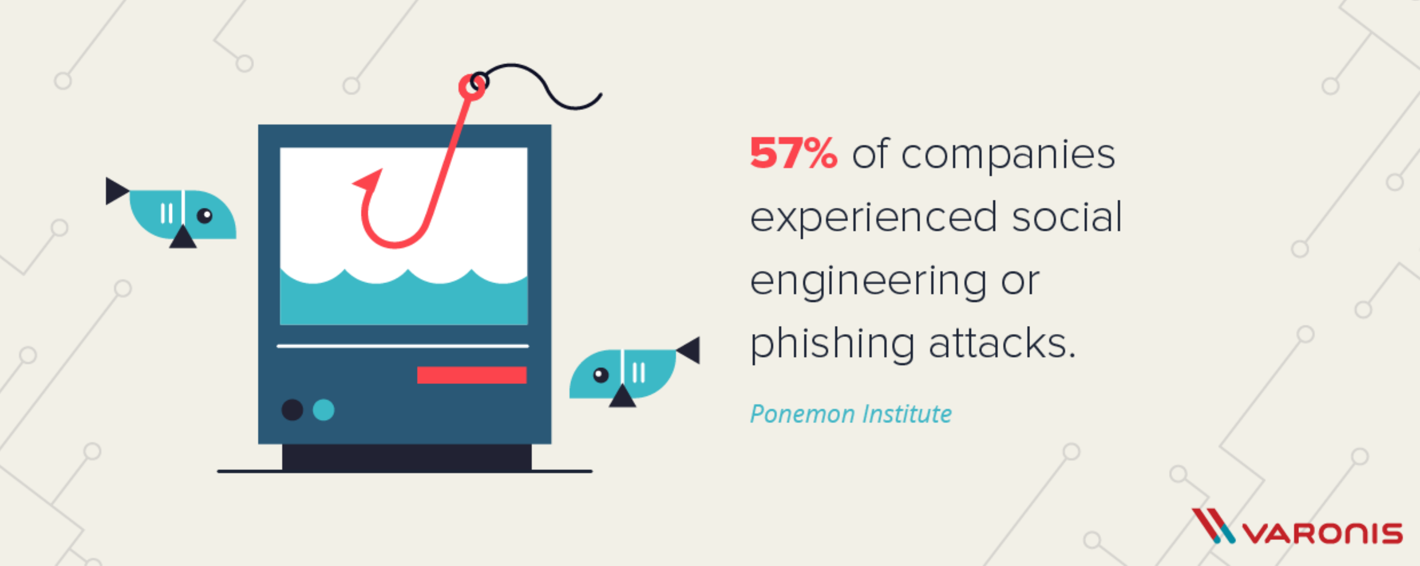
The increasing amount of large-scale, well-publicized breaches suggests that not only are the number of security breaches going up — they're increasing in severity, as well. Data breaches expose sensitive information that often leave exposed users at risk for identity theft, ruin companies' reputations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

12. Security breaches have increased by 11% since 2018 and 67% since 2014. (Accenture)
13. Hackers attack every 39 seconds, on average 2,244 times a day. (University of Maryland)
14. The average time to identify a breach in 2019 was 206 days. (IBM)
15. The average lifecycle of a breach was 314 days (from the breach to containment). (IBM)
16. 500 million consumers, dating back to 2014, had their information compromised in the Marriott-Starwood data breach made public in 2018. (Marriott)
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)
19. The average cost of a data breach is $3.92 million as of 2019. (Security Intelligence)
20. 83% of enterprise workloads will move to the cloud by the year 2020. (Forbes)
21. In 2016, 3 billion Yahoo accounts were hacked in one of the biggest breaches of all time. (NY Times)
22. In 2016, Uber reported that hackers stole the information of over 57 million riders and drivers. (Uber)
23. Uber tried to pay off hackers to delete the stolen data of 57 million users and keep the breach quiet. (Bloomberg)
24. In 2017, 412 million user accounts were stolen from Friendfinder's sites. (Wall Street Journal)
25. In 2017, 147.9 million consumers were affected by the Equifax Breach. (Equifax)

26. The Equifax breach cost the company over $4 billion in total. (Time Magazine)
27. In 2018, Under Armor reported that its "My Fitness Pal" was hacked, affecting 150 million users. (Under Armour)
28. 18 Russians, 19 Chinese individuals, 11 Iranians and one North Korean were involved in indictments for their alleged state-sponsored espionage against the United States. (Symantec)

Cyber Crime Statistics by Attack Type


57% of companies experienced social engineering or phishing attacks.
Ponemon Institute
VARONIS

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, social engineering, Distributed Denial of Service (DDoS) attacks, malware and ransomware.

There are new malware and viruses being discovered every day. Varonis recently discovered the Monero cryptojacking malware during a cryptojacking investigation that secretly plagued a company for over a year.

29. In the 2019 DBIR, 94% of malware was delivered by email. (Verizon)
30. Phishing levels declined, dropping from 1 in 2,995 emails in 2017, to 1 in 3,207 emails in 2018. (Symantec)
31. 34% of data breaches involved internal actors. (Verizon)

32. 51% of businesses experienced denial of service attacks in 2018. (Cybint Solutions)
33. 61% of organizations have experienced an IoT security incident. (CSO Online)
34. Malicious PowerShell scripts blocked in 2018 on the endpoint increased 1,000%. (Symantec)
35. 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)
36. IoT devices experience an average of 5,200 attacks per month. (Symantec)
37. 90% of remote code execution attacks are associated with cryptomining. (CSO Online)
38. The average cost of a ransomware attack on businesses is $133,000. (SafeAtLast)
39. In a different sample, 92% of malware is delivered by email. (CSO Online)
40. 48% of malicious email attachments are office files. (Symantec)
41. 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)
42. Gandcab 5 requires that victims pay $2,499 for the decryption key. (McAfee)
43. 1 in 36 mobile devices had high risk apps installed. (Symantec)
44. In 2018, an average of 10,573 malicious mobile apps were blocked per day. (Symantec)
45. 65% of groups used spear-phishing as the primary infection vector. (Symantec)
46. Mirai distributed denial of service (DDoS) worm remained an active threat and, with 16% of the attacks, was the third most common IoT threat in 2018. (Symantec)
47. 1 in 13 web requests lead to malware. (Symantec)
48. Ransomware detections have been more dominant in countries with higher numbers of internet-connected populations. The United States ranks highest with 18.2% of all ransomware attacks. (Symantec)

49. Most malicious domains, about 60%, are associated with spam campaigns. (Cisco)
50. About 20% of malicious domains are very new and used around 1 week after they are registered. (Cisco)

Cybersecurity Compliance and Governance Statistics

53% of companies had over 1,000 sensitive files open to every employee.
Varonis
VARONIS

With new threats emerging every day, the risks of not securing files is more dangerous than ever, especially for companies. 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 lessons 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.

Try a free risk assessment to see where your vulnerabilities lie.

51. 69% of companies see compliance mandates driving spending. (CSO Online)
52. 53% of companies had over 1,000 sensitive files open to every employee. (Varonis)

53. 22% of all folders were available to every employee. (Varonis)
54. 88% companies spent more than $1 million on preparing for the GDPR. (CSO Online)
55. Google was fined $57 billion for GDPR violations by CNIL, a French data protection agency. (TechCrunch)
56. Companies reportedly spent $9 billion on preparing for the GDPR. (Forbes)
57. By December 2018, only 50% of companies believed they were GDPR compliant. (Data Center Frontier)
58. 15% of companies found 1,000,000+ files open to every employee. (Varonis)
59. 17% of all sensitive files were accessible to all employees. (Varonis)
60. On average, every employee had access to 17 million files. (Varonis)
61. The GDPR fines totaled $63 million in its first year. (GDPR.eu)
62. 1,000 news sources blocked EU readers to avoid the GDPR compliance rules. (Nieman Lab)
63. 61% of companies have over 500 accounts with non-expiring passwords. (Varonis)
64. Businesses spent $1.3 million on average to meet compliance requirements and are expected to put in an additional $1.8 million. (IAAP)
65. Legal advice and teams cost UK FTSE 350 companies about 40% of their GDPR budget or $2.4 million. (Forbes)
66. Since the GDPR was enacted, 31% of consumers feel their overall experience with companies has improved. (Marketing Week)
67. In the GDPR’s first year, there were 144,000 complaints filed with various GDPR enforcement agencies and 89,000 data breaches recorded. (EDPB)
68. Equifax was found liable for their 2017 breach and was fined $425 million by the Federal Trade Commission (FTC) in 2019. (FTC)

Industry-Specific Cyber Stats

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.

69. 43% of breach victims were small businesses. (Verizon)
70. Financial and Manufacturing services have the highest percent of exposed sensitive files at 21%. (Varonis)
71. Financial services had 352,771 exposed sensitive files on average while Healthcare, Pharma and Biotech have 113,491 files on average — the highest when comparing industries. (Varonis)
72. 15% of breaches involved Healthcare organizations, 10% in the Financial industry and 16% in the Public Sector. (Verizon)
73. The banking industry incurred the most cybercrime costs in 2018 at $18.3 million (Accenture)

74. Smaller organizations (1–250 employees) have the highest targeted malicious email rate at 1 in 323. (Symantec)
75. WannaCry ransomware attack cost the National Health Service (NHS) over $100 million. (Datto)
76. The estimated losses in 2019 for the healthcare industry are $25 billion. (SafeAtLast)
77. Lifestyle (15%), and Entertainment (7%) were the most frequently seen categories of malicious apps. (Symantec)
78. Supply chain attacks are up 78% in 2019. (Symantec)
79. Trojan horse virus Ramnit largely affected the financial sector in 2017, accounting for 53% of attacks. (Cisco)
80. The financial services industry takes in the highest cost from cybercrime at an average of $18.3 million per company surveyed. (Accenture)
81. The industry with the highest number of attacks by ransomware is the healthcare industry. Attacks will quadruple by 2020. (CSO Online)

Security Spending and Cost Statistics

Average expenditures on cybercrime are increasing dramatically, and costs associated with these crimes can be crippling to companies who have not made cybersecurity 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.

82. By 2020, security services are expected to account for 50% of cybersecurity budgets. (Gartner)
83. The average cost of a malware attack on a company is $2.6 million. (Accenture)
84. $3.9 million is the average cost of a data breach. (IBM)
85. Healthcare had the highest data breach costs at $429 per record. (IBM)
86. The average cost per record stolen is $150. (IBM)
87. The total cost of cybercrime for each company increased by 12% from $11.7 million in 2017 to $13.0 million in 2018. (Accenture)
88. The average annual security spending per employee doubled, from $584 in 2012 to $1,178 in 2018. (Gartner)
89. The cost of lost business averaged $1.42 million. (IBM)
90. The average cost in time of a malware attack is 50 days. (Accenture)
91. The most expensive component of a cyber attack is information loss at $5.9 million. (Accenture)
92. The average cost per lost or stolen records per individual is $141 — but that cost varies per country. Breaches are most expensive in the United States ($225) and Canada ($190). (Ponemon Institute’s Cost of Data Breach Study)
93. In companies with over 50k compromised records, the average cost of a data breach is $6.3 million. (Ponemon Institute’s Cost of Data Breach Study)
94. Including turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill, the cost of lost business globally was highest for U.S. companies at $4.13 million per company. (Ponemon Institute’s Cost of Data Breach Study)
95. Damage related to cybercrime is projected to hit $6 trillion annually by 2021. (Cybersecurity Ventures)

96. Ransomware damage costs will rise to $11.5 billion in 2019 and a business will fall victim to a ransomware attack every 14 seconds at that time. (Cybersecurity Ventures)

97. The United States and the Middle East spend the most on post-data breach response. Costs in the U.S. were $1.56 million and $1.43 million in the Middle East. (Ponemon Institute’s 2017 Cost of Data Breach Study)

98. 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)

Cybersecurity Job Statistics

The demand for cybersecurity professionals continues to rise along with the rates of attacks and increases in cybersecurity budgets. The imbalance of the amount of skilled cybersecurity workers along with the high demand to fill cybersecurity positions has caused a cybersecurity skills shortage.

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.

99. 82% of employers report a shortage of cybersecurity skills. (ISSA)

100. 61% of companies think their cybersecurity applicants aren't qualified. (ISSA)
101. The cybersecurity unemployment rate is 0% and is projected to remain there through 2021. (CSO Online)
102. It's predicted that by 2021, 100% of large companies globally will have a CISO position. (Cybersecurity Ventures)
103. By 2021, it's projected that there will be 3.5 million unfilled cybersecurity jobs globally. (Cybersecurity Ventures)
104. Information Security Analysts job positions in the US are expected to grow 32% from 2018–28. (Bureau of Labor Statistics)
105. Computer Network Architect job positions in the US are expected to grow 5% from 2018–28. (Bureau of Labor Statistics)
106. Computer Programmer job positions in the US are expected to decline 7% from 2018–28. (Bureau of Labor Statistics)
107. Since 2016, the demand for Data Protection Officers (DPOs) has skyrocketed and risen over 700%, due to the GDPR demands. (Reuters)
108. 500,000 Data Protection Officers are employed (IAAP)
109. 66% of cybersecurity professionals struggle to define their career paths. (ISSA)
110. 60% of cybersecurity professionals aren't satisfied with their current job. (ISSA)

Below is a visual guide of some of the most important facts and figures that shape the cybersecurity field.

Interested to see how the landscape has changed? Click the button below to see our 2019 visual data compilation.

Cybersecurity Statistic FAQs

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

Q: What's the Biggest Cybersecurity Threat to Businesses?

A: 56% of IT decision-makers believe phishing attacks are their top security threat. 32% of breaches involved phishing — phishing awareness and education are some of the best ways to decrease risk.

Q: What Are the Most Common 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 Cyber Attacks Happen a Day?

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

8 Cybersecurity Statistics Reports

Below are some helpful cybersecurity studies and articles to deepen your knowledge about the cybersecurity landscape.

- Accentures's 2019 Cost of Crime Study
- Cisco's Cybersecurity Reports
- Cybersecurity Venture's Job Study
- Symantec 2019 Internet Security Threat Report
- RiskBased Mid-Year Data Breach Report
- Varnois' 2019 Data Risk Report
- Verizon's 2019 Data Breach Investigations Report
- World Economic Forum's 2019 Global Risk 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. 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.

RELATED POSTS

DATA SECURITY

Threat Update #15 – Thanksgiving Special Edition

DATA SECURITY, INCIDENT RESPONSE

Threat Update #14 – Post-Ransomware Recovery

DATA SECURITY

What is Role-Based Access Control (RBAC)?

CYBERSECURITY NEWS, DATA SECURITY, THREAT DETECTION

Watch: Varonis ReConnect! Defending Against Today’s Spookiest Malware

Français
Deutsch
日本語
Русский
Português

SOLUTIONS
Remediation & Governance
Security Analytics
Data Classification
Ransomware
Insider Threats
External Threats

PLATFORM
How It Works
How to Buy
How to Use It
Real Results
ROI
Integrations

COMPANY
About Varonis
Varonis Life
Careers
Customers
Investor Relations
Brand
Contact Us

RESOURCES
Free Security Training
Analyst Reports
Whitepapers
Guides
Videos
Events

PARTNERS
Technology Partners
Channel Partners
Partner Portal