UNITRENDS
A Kaseya COMPANY

The unprecedented rate of technology adoption has exceeded many organizations' ability to identify, manage and mitigate the risks associated with these technologies. The threat vectors opened by remote workforces, cloud-based technologies and IoT present new and unforeseen challenges. Data breaches and cyberattacks are reaching new heights with regards to their efficacy and organizational impact.

The Impact of a Data Breach

$4.88 MILLION

The average cost of a data breach increased by 10% in 2024, reaching $4.88 million, compared to $4.45 million in 2023. This rise was largely due to business disruptions and expenses related to post-breach responses.[1]

85% OF KNOWN VULNERABILITIES

- remain unremedied 30 days after a patch was made available. It takes about 55 days to fix half of the most serious security issues after a solution is available. Most patches don't even begin until 30 days later, and by the end of the year, around 8% of these vulnerabilities are still not fixed.[2]

292 DAYS

- to identify and contain a breach involving stolen credentials. Cyberattacks that trick employees or misuse their access also took a long time to resolve. For instance, phishing attacks took an average of 261 days to resolve, while other scams designed to manipulate employees took about 257 days to fix.[3]

Key Factors Fueling Data Breaches

According to 99% of companies that fell victim to ransomware, exploitation of security vulnerabilities and malicious emails were the top two root causes of cyberattacks.[4] Phishing is often the first step in stealing login details, which can then be used for further attacks.

Notable Breaches in Recent Years

73 MILLION CUSTOMERS IMPACTED

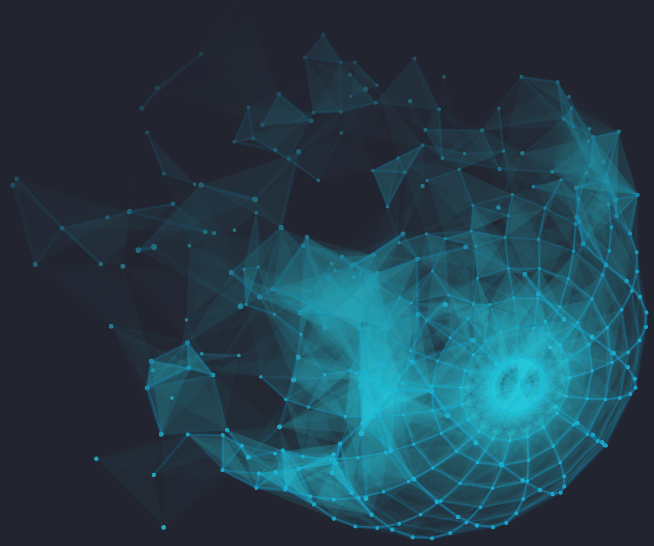
In March 2024, AT&T, a leading American telecommunications corporation, announced a major security breach in which hackers leaked sensitive customer information on the dark web. The compromised data included personal details such as names, email addresses, dates of birth, and Social Security numbers. This breach affected 73 million individuals, including both current and former customers.[5]

560 MILLION CUSTOMERS DATA BREACHED

In May 2024, Ticketmaster experienced a large-scale cyberattack when hackers exploited a vulnerability in a third-party cloud system. This breach exposed sensitive customer information, including names, email addresses, payment information and ticket purchase histories, impacting around 560 million users.[7] Following the breach, the attackers attempted to sell the stolen information on dark web forums.

OVER 2,600 ORGANIZATIONS AND 77 MILLION INDIVIDUALS AFFECTED

In 2023, a critical vulnerability was discovered in the MOVEit software, a widely used file transfer tool. Cybercriminals exploited the flaw to gain unauthorized access to sensitive data.[6] The attackers then engaged in data extortion, threatening to release the stolen information unless their ransom demands were met. This incident affected businesses, government agencies and millions of individuals across various sectors.



Cost of a Data Breach

Risks of a Data Breach

Today, an organization's data lives in multiple environments — on-premises data centers, private clouds, public clouds and hybrid clouds. With critical data scattered in multiple places, data protection has become increasingly complex and challenging. According to the Cost of a Data Breach Report 2024, around 40% of data breaches involved information spread across various environments.[8]

- LOSS OF SENSITIVE DATA
- FINANCIAL LOSSES
- REPUTATIONAL DAMAGE
- OPERATIONAL DOWNTIME
- LEGAL FEES & REGULATORY PENALTIES

DOWNLOAD OUR EBOOK TO LEARN MORE ABOUT THE KEY THINGS TO CONSIDER WHEN SELECTING THE RIGHT BCDR SOLUTION FOR YOUR ORGANIZATION.

DOWNLOAD THE EBOOK

Sources
1, 3, 8 https://www.ibm.com/reports/data-breach
2 https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf
4 https://www.sophos.com/en-us/content/state-of-ransomware
5 https://about.att.com/story/2024/addressing-data-set-released-on-dark-web.html
6 https://www.csoonline.com/article/1248857/moveit-carnage-continues-with-over-2600-organizations-and-77m-people-impacted-so-far.html
7 https://www.bitdefender.com/blog/hotforsecurity/notorious-hacking-group-claims-ticketmaster-data-breach-personal-details-of-560-million-customers-potentially-compromised/?srsltid=AfmBOooafmgDXbjgzADFsZBgmfgDreeTUzotBijfutBrcY68z_yivL4C%2F

ABOUT UNITRENDS

Unitrends makes efficient, reliable backup and recovery as effortless and hassle-free as possible. We combine deep expertise gained over 30 years of focusing on backup and recovery with next-generation backup appliances and cloud purpose-built to make data protection simpler, more automated and more resilient than any other solution in the industry.

UNITRENDS
A Kaseya COMPANY

22102024