BioSpectrum ASIA EDITION
the business of Bio & Health Sciences

Varonis releases 2021 report on Healthcare Data Risk

April 7, 2021 | News

Healthcare remains one of the most at-risk sectors for malicious attacks in 2021



Varonis, a global pioneer in data security based in the US, has just released its 2021 Healthcare Data Risk Report, which delves into the state of data security in hospitals, pharmaceutical firms, and biotechnology companies.

Recent attacks against the healthcare and biotech sector demonstrate maliciousness on an unprecedented scale. While their methods vary, their goal is the same: grab sensitive data to steal, sell, or extort.

Healthcare remains one of the most at-risk sectors for malicious attacks in 2021, with COVID-19 enabling hackers to take advantage of organisations on the front lines. In the last year, cybercriminals have unleashed potent variants of ransomware like Maze and Ryuk on hundreds of hospitals, and state-sponsored actors zeroed in on pharma and biotech companies to harvest COVID-19 research.

The healthcare industry was woefully underprepared for cyber attacks in 2020, with an average breach lifecycle of 329 days — the highest of any industry — and an average data breach cost of $7.13 million in 2020 — a 10.5% increase over 2019. 2020 also marked the first year that a patient's death has been directly linked to a cyberattack.

Some of the key findings in the report which provide an alarming picture of overexposed and vulnerable sensitive data include:

- 1 in 5 files are open to every employee in healthcare organisations on average. This increases to 1 in 4 in small and mid-sized organisations.
- The average organisation has 31,000 sensitive files (those containing HIPAA + financial + proprietary research) open to everyone, on average.
- 77% of organisations have 500+ accounts with passwords that never expire.
- Every healthcare employee has access to over 11 million files overall — all it takes it one account to be compromised to let a hacker in.