



April 25, 2017

## 47% of Organizations Had at Least 1,000 Sensitive Files Accessible to Every Employee, Reveals Varonis Data Risk Report

### Stale data and excessive employee permissions continue to expose organizations to insider threats, ransomware and other risks

NEW YORK, April 25, 2017 (GLOBE NEWSWIRE) -- [Varonis Systems, Inc.](#) (NASDAQ:VRNS), a leading provider of software solutions that protect data from insider threats and cyberattacks, today revealed the results from the [Varonis Data Risk Report](#), showcasing an alarming level of exposure for corporate and sensitive files across organizations, including an average of 20% of folders per organization open to every employee.

Using the Varonis Data Security Platform (DSP), Varonis conducted over a thousand risk assessments for customers and potential customers on a subset of their file systems. The assessment provides insight into the risks associated with corporate data, identifies where sensitive and regulatory data resides, reveals over-exposed and high risk areas, and makes recommendations to increase their data security posture.

Additional key findings from the report include:

- | 236.5 million folders containing 2.8 billion files, comprising 3.79 petabytes of data were analyzed.
- | Of that figure, 48,054,198 folders were open to "global access groups," or groups that grant access to the entire organization.
- | 47% of organizations had at least 1,000 sensitive files open to every employee; 22% had 12,000 or more sensitive files exposed to every employee.
- | 71% of all folders contained stale data, accounting for almost 2 petabytes of data.
- | 24.4 million folders had unique permissions, increasing complexity and making it more difficult to enforce a least privilege model and comply with regulations like General Data Protection Regulation (GDPR).

Failure to reduce the use of global access groups, lock down sensitive files and dispose of stale data exposes an organization to data breaches, insider threats and crippling ransomware attacks. A [recent Ponemon study](#) found that 62% of end users say they have access to company data they probably should not see, and a [Forrester Consulting study](#) found that 59% don't enforce a need-to-know permissions model for sensitive files.

Individual company risks identified during the assessments include:

- | 35% of an insurance firm's 86.4 million folders were open to every employee.
- | 80% of a banking institution's 245,575 sensitive files were accessible to every employee.
- | Another banking institution had 11.6 million folders with unique permissions, complicating its efforts to reduce file access on a need-to-know basis.

"In data breaches and ransomware attacks, files are targeted because they are high value assets and usually vulnerable to misuse by insiders and outsiders that transgress the perimeter. While organizations focus on outer defenses and chasing threats, the data itself is left broadly accessible and unmonitored," said Ken Spinner, VP of Field Engineering at Varonis. "Organizations participate in our risk assessments because they understand the value of their data and the risk it poses for being stolen or abused. We applaud their efforts in taking the first step towards mitigating risk."

"We found files with sensitive PII in places it should not have been," said a [Chief Security Officer](#) for a state and local government in a recent [TechValidate customer survey](#).

According to that same survey, [68% of end users perform](#) a risk assessment to validate security concerns, [95% agree](#) that the risk assessment helped them identify at-risk, sensitive and classified data and build a plan of attack to reduce the likelihood of a data breach, and [82% rate](#) global access remediation a top priority after seeing the results.

"The initial assessment gets the immediate attention of management, which then assists in building and executing the internal remediation process," said a [Security Manager](#) at a beverage company in the same TechValidate customer survey. "Varonis does an excellent job of identifying internal data security vulnerabilities."

The Varonis Data Risk Report showcases the findings from a random sampling of 80 risk assessments conducted for customers and potential customers between January to December of 2016 across 12 countries and 33 industries, and within organizations with 50 to more than 10,000 employees. All organizational identifiers have been removed.

### **Additional Resources**

- | Read the full Data Risk Report: [www.varonis.com/data-risk-report-2017](http://www.varonis.com/data-risk-report-2017).
- | See why organizations perform a risk assessment and the benefits they receive: [www.techvalidate.com/portals/why-organizations-perform-a-varonis-risk-assessment](http://www.techvalidate.com/portals/why-organizations-perform-a-varonis-risk-assessment).
- | For more information on Varonis' solution portfolio, please visit [www.varonis.com](http://www.varonis.com).
- | Visit our [blog](#), and join the conversation on [Facebook](#), [Twitter](#), [LinkedIn](#), [Podcast](#) and [YouTube](#).

### **About Varonis**

Varonis is a leading provider of software solutions that protect data from insider threats and cyberattacks. Through an innovative software platform, Varonis allows organizations to analyze, secure, manage, and migrate their volumes of unstructured data. Varonis specializes in file and email systems that store valuable spreadsheets, word processing documents, presentations, audio and video files, emails, and text. This rapidly growing data often contains an enterprise's financial information, product plans, strategic initiatives, intellectual property, and confidential employee, customer or patient records. IT and business personnel deploy Varonis software for a variety of use cases, including data security, governance and compliance, user behavior analytics, archiving, search, and file synchronization and sharing. With offices and partners worldwide, Varonis had approximately 5,350 customers as of December 31, 2016, spanning leading firms in financial services, healthcare, public, industrial, insurance, energy and utilities, media and entertainment, consumer and retail, technology and education sectors.

News Media Contact:  
Jennifer LuPiba  
614-338-9889  
[jlupiba@varonis.com](mailto:jlupiba@varonis.com)