COMPLIANCE BRIEF: VARONIS AND THE US SECURITY AND EXCHANGE COMMISSION'S OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS (SEC OCIE)

OVERVIEW

The SEC's Office of Compliance Inspections and Examinations (OCIE)'s cybersecurity initiative is responsible for assessing and preparing for cybersecurity threats in the securities industry. As part of this initiative, the OCIE will conduct more than 50 cybersecurity exams for registered broker-dealers and investment advisors. These examinations will help identify areas where the Commission and the industry can work together to protect investors and capital markets from cybersecurity threats.

Mapping Risk Alerts to Varonis

The OCIE's Risk Alert Appendix sheet is designed to empower industry professionals with questions they can use to assess their firms' level of preparedness, regardless of the questions that are included in OCIE's exams. The following is a table containing sections of the Risk Alert Appendix and (where applicable) an explanation describing how Varonis solutions can help.

Risk Alerts Appendix	Description	Varonis Solutions
Identification of Risks	○ Maps of network resources, connections, and data flows (including locations where customer data is housed) are created or updated.	The Varonis IDU Classification Framework can scan the environment for data shares, and inventory and classify data on network resources (file servers, intranets, etc.) to determine where customer data resides. The DatAdvantage audit trail provides a complete record of file and email flows: creates, deletes, moves, modifies, sends, receives, etc.
	○ Resources (hardware, data, and software) are prioritized for protection based on their sensitivity and business value.	The IDU Classification Framework identifies the highest concentrations of sensitive data that are most at risk and provides a clear methodology to safely remediate that risk without manual effort. The Varonis IDU Classification Framework allows organizations to crawl their file systems looking for regulated content as well as data that matches known sensitive patterns, such as credit card numbers, social security numbers, project names, client names, critical projects, etc. Use DatAdvantage to run reports to identify, prioritize, and remediate excessive access to sensitive,high-risk data.

	○ Logging capabilities and practices are assessed for adequacy, appropriate retention, and secure maintenance.	**Auditing and Logging** Varonis DatAdvantage monitors every user's file touch and stores in a searchable format, all aspects of data use for information stored on file servers and Network Attached Storage (NAS) devices. Varonis DatAlert can alert when in real time when inappropriate activities take place (changes made outside change control windows, etc.) **Data Retention** Varonis DTE provides the flexibility to configure complete end-to-end migration rules: define source criteria based on path, and/or content, classification rule, Varonis ownership and follow-up (flag/ tag) criteria, define destination path, folder, and permissions translation, and when the migration will take place. The ability to configure these rules allow for the rapid and safe execution of complex data migrations, and to easily implement and enforce policies for data retention and location based on content, accessibility, and activity.
Protection of Firm Networks and Information	The Firm provides written guidance and periodic training to employees concerning information security risks and responsibilities. If the Firm provides such guidance and/or training, please provide a copy of any related written materials (e.g., presentations) and identify the dates, topics, and which groups of employees participated in each training event conducted since January 1, 2013.	Varonis staff are also avid learners and educators. Here are some of the educational opportunities we offer and provide: ○ Professional Services: ensures our customers can effectively assess and remediate risks and maintain a secure environment. ○ Varonis Blog: learn more about security, privacy, IT Operations and more on our blog. We post approximately 3-4 blog posts per week Office Hours: 1 free hour one-on-one live web session with your local Engineer to discuss operational and security questions.

The Firm maintains controls to prevent unauthorized escalation of user privileges and lateral movement among network resources. If so, please describe the controls, unless fully described within policies and procedures.

The Firm restricts users to those network resources necessary for their business functions. If so, please describe those controls, unless fully described within policies and procedures.

The Firm has a process to manage IT assets through removal, transfers, and disposition.

DatAdvantage recommends the revocation of permissions to data for those users who do not have a business need to the data – this ensures that user access to data is always warranted and driven by *least privilege*.

DatAdvantage generates reports showing the history of permission revocations and the percentages by which overly permissive access was reduced.

DataPrivilege provides a mechanism via a web-based application by which to monitor, administer (allow/deny) all access requests to unstructured data and membership in administrative groups.

DatAlert can send real-time notifications when a user is granted super-user or administrative access.

Data Transport Engine provides a means for IT to setup policies for when data should be moved, archived, or deleted. Criteria can be based on staleness, size, location, sensitivity, and more, making defensible disposition and data retention policies possible to enforce.

Risks Associated With Vendors and Other Third Parties	If vendors, business partners, or other third parties may conduct remote maintenance of the Firm's networks and devices, describe any approval process, logging process, or controls to prevent unauthorized access, and provide a copy of any relevant policies and procedures.	DataPrivilege automates entitlement reviews so that contractor and other 3rd party accounts may be reviewed regularly. Expiration dates may also be set to automatically revoke access upon termination of their contract. DatAnywhere instantly enables mobile access, file synchronization, and **secure 3rd party sharing** for your existing file shares. Files can stay exactly where they are—on existing SMB file servers or NAS. Third party access is monitored and can be revoked at any time. Third party links can contain expiration dates and pin codes for extra security and can be revoked at any time. Third parties **do not** require an entry in the organizations Active Directory or LDAP system. **Private cloud benefits:** ○ Definitive copies of files are always stored on corporate storage ○ No one gets permissions to shared data unless they already have it ○ Users authenticate to Active Directory or LDAP and there is no need to reconfigure or replicate permissions ○ IT controls speed, availability, and security

Detection of Unauthorized Activity	Identifying and assigning specific responsibilities, by job function, for detecting and reporting suspected unauthorized activity. Aggregating and correlating event data from multiple sources. Establishing written incident alert thresholds.	**Data Breaches and Monitoring** Varonis DatAlert provides real-time alerting based on file activity, Active Directory changes, permissions changes, and other events from all major unstructured data platforms. Alert criteria and output are easily configurable so that the right people and systems can be notified about the right things, at the right times in the right ways. DatAlert improves your ability to detect possible security breaches, and misconfigurations.

ABOUT VARONIS

Varonis is the leading provider of software solutions for unstructured, human-generated enterprise data. Varonis provides an innovative software platform that allows enterprises to map, analyze, manage and migrate their unstructured data. Varonis specializes in human-generated data, a type of unstructured data that includes an enterprise's spreadsheets, word processing documents, presentations, audio files, video files, emails, text messages and any other data created by employees. This data often contains an enterprise's financial information, product plans, strategic initiatives, intellectual property and numerous other forms of vital information. IT and business personnel deploy Varonis software for a variety of use cases, including data governance, data security, archiving, file synchronization, enhanced mobile data accessibility and information collaboration.

FREE 30-DAY ASSESSMENT

WITHIN HOURS OF INSTALLATION

You can instantly conduct a permissions audit: File and folder access permissions and how those map to specific users and groups. You can even generate reports.

WITHIN A DAY OF INSTALLATION

Varonis DatAdvantage will begin to show you which users are accessing the data, and how.

WITHIN 3 WEEKS OF INSTALLATION

Varonis DatAdvantage will actually make highly reliable recommendations about how to limit access to files and folders to just those users who need it for their jobs.

START YOUR FREE TRIAL

WORLDWIDE HEADQUARTERS
1250 Broadway, 31st Floor, New York, NY 10001 T 877-292-8767 **E** sales@varonis.com **W** www.varonis.com

UNITED KINGDOM AND IRELAND
Varonis UK Ltd., Warnford Court, 29 Throgmorton Street, London, UK EC2N 2AT T +44 0207 947 4160 **E** sales-uk@varonis.com **W** www.varonis.com

WESTERN EUROPE
Varonis France SAS, 13-15 rue Jean Jaures (1er Etage) 92800 Puteaux T +33 184 88 56 00 **E** sales-france@varonis.com **W** sites.varonis.com/fr

GERMANY, AUSTRIA AND SWITZERLAND
Varonis Deutschland GmbH, Welserstrasse 88, 90489 Nürnberg T +49(0) 911 8937 1111 **E** sales-germany@varonis.com **W** sites.varonis.com/de