COMPLIANCE BRIEF: VARONIS AND THE FINANCIAL CONDUCT AUTHORITY

BACKGROUND

In April of 2007 the Financial Crime and Intelligence Division (FCID) of the Financial Services Authority (FSA) conducted a survey to gauge how well UK financial services firms of all sizes understand their data security risks and learn what steps they've taken to mitigate the risks associated with customer data in their care. The results were published in Data Security in Financial Services: Firms' controls to prevent data loss by their employees and third party suppliers. Based on the research, the report included a list of recommended practices and controls for all financial firms, but with a special focus on smaller enterprises.

In 2013, the FSA was split into two bodies, the Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA). The FCA regulates financial service firms from a conduct perspective; the PRA, now a subsidiary of the Bank of England, regulates only insurers and deposit taking institutions. The FCA has taken over the former FSA's financial crime functions, as well as consumer data protection oversight.

Who Needs To Comply

While the FCA does not offer the Date Security in Financial Services report as part of its formal guidance to UK financial services firms, it does expect that the findings and best practices contained in the report are translated into more effective controls and processes by which firms improve the security posture of customer data for which they are responsible. The FCA reserves the right to take enforcement action with firms that do not show an improvement in conducting risk assessments and mitigation as of the issuance of the report.

What Are The Risks Of Non-Adherence?

The report's findings indicate very clearly that UK financial services firms' current practices for data protection are poor. This puts customer data at serious and high risk from theft, loss or misuse. The status quo means potential increases in financial crime including identity fraud and theft. Such an increase means significant detriment to individuals who must invest time and resources to repairing damaged credit or retrieving lost funds. It also means loss of market and citizen confidence in the financial services firm that suffers the breach therefore impacting that firm's reputation and revenues for the long term.

How Varonis Can Help With FCA Best Practice Adherence?

Varonis provides a comprehensive system for meeting the "good practices" put forth by the former FSA's Financial Crime and Intelligence Division (FCID) for unstructured data, that is, the contents of file servers. In particular, Varonis solutions ensure that access and use of sensitive and important financial and customer information residing on file servers is automatically ratcheted down to business need-to-know, and that use of sensitive data is continuously monitored so that organizations have an accurate audit data use and user access behavior at all times.

Specifically, Varonis has created a suite comprised of two products which, when taken together, furnish a complete framework for managing, securing and reporting on all aspects of unstructured data use. They are: DatAdvantage and DataPrivilege.

VARONIS DATADVANTAGE

The Varonis DatAdvantage software solution aggregates user, data and access event information from directories and file servers. Sophisticated analytics applied to the collected information show detailed data use and determine rightful access based on business need. Specifically, and in a non-intrusive way, Varonis:

- Protects data by recommending removal of overly permissive access controls
- Restricts unstructured data access to those with a business need for that data
- Tracks and monitors every user's every file touch
- Re-computes access controls to account for changes in roles and file server contents

VARONIS DATAPRIVILEGE

DataPrivilege makes it possible to transition the responsibility of data entitlement management from IT to business owners without any infrastructure changes or business disruption. DataPrivilege brings together data owners and data users in a forum for communicating, authorizing and activating entitlements. Varonis DataPrivilege allows you to implement a cohesive data entitlement environment, thereby raising accountability and reducing risk. Upon implementation, DataPrivilege provides:

- Data protection by reducing errors in entitlement management
- Business need-to-know access control by enabling data owners to make the call
- Access approval rationale capture for refinement and improvement
- Policy and workflow enforcement for consistency and greater security

Mapping FCA Best Practices to Varonis Functionality

FSA Good Practice	Description	Varonis Functionality
Governance (3.1.7)	Identifying data security as a key specific risk, subject to its own governance, policies and procedures and risk assessment.	Varonis DatAdvantage provides summary dashboards that aid in determining the risk posture of unstructured data sets. For instance, for any given folder administrators can see the percent of permissions that are assigned (relative to the) percent that have been removed or are earmarked for removal. This relationship essentially shows how much risk has been reduced for that folder. The dashboards are routinely updated so that the risk posture or percent of assigned access permissions can be compared in time.
	A senior manager with overall responsibility for data security, specifically mandated to manage data security risk assessment and communication between the key stakeholders within the firm such as: senior management, information security, human resources, financial crime, security, IT, compliance and internal audit.	Varonis DatAdvantage and DataPrivilege enable complete management of the workflow and enforcement of authorizations to data. Business owners are defined within the application as are the data sets (i.e. files and folders) to which they are responsible. All user requests to data are processed automatically by the DataPrivilege application as are the "allow" or "deny" decisions the permissions level (i.e. read, write, modify) and the expiry (i.e. valid for 30 –days). This increases the accountability of persons for data access controls while limiting that capability to the right parties for a given data set. Most importantly it enables timely communication and coordination among data stakeholders about entitlement privileges and unstructured data use. Compliance auditors and executive sponsors can also monitor the process and progress of granting and revoking access.

Access Rights (3.4.2)	Specific IT access profiles for each role in the firm, which set out exactly what level of IT access is required for an individual to do their job.	With Varonis DataPrivilege organizations can define access policies to unstructured data that are commensurate with the user's business role. The application will enforce a workflow for requesting and granting access to file share data. It will also ensure that the permissions and revocations are applied per the expressed policy. The entire process and rationale for granting and revoking access can be audited by compliance officers and stakeholders from within DataPrivilege. The activity is also captured in reports for future scrutiny and as part of an audit record.
	When a staff member changes roles or responsibilities, all IT access rights are deleted from the system and the user is set up using the same process as if they were a new joiner at the firm. The complexity of this process is significantly reduced if role-based IT access profiles are in place – the old one can simply be replaced with the new.	Varonis DatAvantage provides the only known (patent-pending) means to programmatically compute the user to data mapping thereby automating the continuous enforcement of least-privilege access. By recommending revocations the application ensures that only the right users are getting to the right data on file shares at all times through data growth as well as changes in user roles, responsibilities and needs to data. Further, the companion application DataPrivilege, automates to process of user access requests and data access authorizations and revocations. This has a marked increase in overall security through improvement in the timeliness and accuracy with which controls are applied.
	A regular reconciliation of HR and IT user records to act as a failsafe if the firm's leavers process fails.	All audit records of user access events to unstructured data and administrator activity on the file system are time stamped and kept as part of the detailed audit log that Varonis DatAdvantage maintains.

	Regular reviews of staff IT access rights to ensure there are no anomalies.	Varonis provides full visibility to the access permissions to unstructured data and folders as set. It also presents a detailed log of how users are using those privileges to access data and how. Overly rigorous access to a data set will generate an alert along with a report of that user's activity, both of which will be sent as notification to the subscribers of that report and those alerts (i.e. IT)
	Least-privilege access to call recordings and copies of scanned documents obtained for 'know your customer' purposes.	As mentioned above, Varonis DatAdvantage maintains timely application of least privilege access controls by continuously monitoring user access to unstructured data including documents and multi-media files, and generating a list of users whose access to unstructured data should be revoked based on lack of business need.
Monitoring Access To Customer Data (3.4.4)	Risk-based, proactive monitoring of staff's access to customer data to ensure that it is being accessed and/or updated for a genuine business reason.	Varonis aids in conducting routine security assessments of file share contents. Administrators of file share contents can see who has permissions to data and who is using those permissions to access data and how (i.e. open, delete, create, rename). Administrators can query the database by person, group or data set of interest by action taken and time period or any combination thereof.

Using software designed to spot suspicious activity by employees with access to customer data. Such software may not be useful in its 'off-the-shelf' format so it is good practice for firms to ensure it is tailored to their business profile.	Because Varonis maintains a detailed history of user activity to unstructured data on file systems, the DatAdvantage application makes note of what is a mean or normal level of access for individuals. And since access is continually monitoring if anomalous access activity is observed (i.e. above the mean) an alert is generated and a report of that user's detailed access activity is sent to the appropriate parties. Examples of anomalous activity might indicate individuals who are accessing the file shares in order to retrieve large amounts of data for to take with them upon terminating their employment. Also, infected workstations and laptops may be house scripts which register an inordinate number of file opens or deletes. Consequently, anomalous or overly rigorous access activity by individuals to file share data will trigger an alert and the generation of an access activity report.
Strict controls over superusers' access to customer data and independent checks of their work to ensure they have not accessed, manipulated or extracted data that was not required for a particular task.	Varonis DatAdvantage maintains a detailed history of all objects managed by the Varonis application including users, user groups and by extension administrative accounts within user directories. At any given time users of DatAdvantage can generate reports that show which administrators changed security settings and access permissions to file servers and their contents. The same level of detail is provided for users of data, showing their access history as well as any changes made to security and access control setting of files and folders.

Internal Audit and Compliance Monitoring (3.8.2)	Compliance and internal audit conducting specific reviews of data security which cover all relevant areas of the business including IT, security, HR, training and awareness, governance and third-party suppliers.	With Varonis organizations can conduct data security reviews at will and generate access reports with a mouse click. This information can focus narrowly on data of a particular type or access by a particular group or it can focus broadly on access activity trends for the organization (i.e. active users, inactive users, active data, stale data, data business ownership reports etc.) Because Varonis maintains a history on all objects every user and every piece of data and the changes to that entity's access levels are noted and maintained. Changes from one reporting cycle to the next are also pre-packaged by default as part of the reporting module functions. Changes to either the access controls or security settings of the file system are noted in a delta report, which can be sent to the appropriate parties as required (i.e. daily, weekly, monthly etc.) The rich audit log provided with Varonis DatAdvantage.

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