COSMOS
Navigate the Compliance Universe

CEP Magazine - April 2019
The CCO's blind spot: When team members go online

By John Klassen

John Klassen (jklassen@authentic8.com) is a Product Marketing Manager at Authentic8 in Redwood City, CA, USA.

- *linkedin.com/in/johnkklassen*

Investment management firms depend on the internet for research, web apps, and communication with business partners, and most firms rely on the web browser as a primary tool for conducting business. This has created a widening compliance blind spot, because locally installed web browsers are notoriously difficult to maintain, secure, and monitor. How can chief compliance officers (CCOs) and IT teams manage the associated risks?

What happens when employees go online? Behind closed doors, many CCOs and IT administrators readily admit they don't really know. Most compliance teams have only limited visibility into their employees' online behavior. Though diligent about archiving email and chat communications, their firms lack similar records of employee web activities.

Finding themselves under growing pressure from regulators to ensure compliance and remediate areas of cybersecurity weakness,[1] compliance officers cannot trust that tightening policies and updating compliance handbooks will be sufficient to protect the firm and satisfy examiners.

Control lost, risk increased

Compliance leaders and IT administrators have ample reason to worry. Without effective governance and granular oversight of employee activities online, regulated firms are facing increasing risks of noncompliant behavior and cybersecurity breaches, mainly in three areas:

- **Social media and online comments/reviews:** Social media sites are of particular concern for a growing number of CCOs.[2] Employees posting public online comments run the risk of violating the Testimonial Rule.[3] This risk extends well beyond the "traditional" social media sites; infractions are as likely to happen on LinkedIn or Facebook as in the comment sections of industry portals or garden-variety investor blogs.
- **Data exfiltration by insiders:** Regular web browsers allow for unrestricted—and unmonitored—copy/paste or file transfer, for example from one cloud storage account or service to another.
- **Remote access and personal devices (BYOD):** Employees are accessing sensitive data from remote locations like a home office, coffee shop, or airport lounge, often from insufficiently protected hardware, and they can inadvertently compromise the firm's network in the process.

How did firms lose control and visibility over such critical areas? Industry insiders blame the web browser.[4] The primary tool used by employees in their online activities has become a critical compliance blind spot.