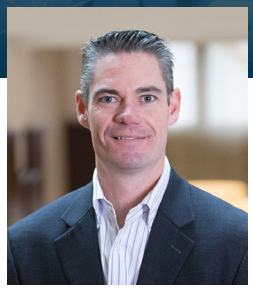
Data Security Considerations for Companies with a Remote Workforce

JULY 2020

by Sean Tuttle and Daniel Fuller



Sean Tuttle
Partner, StoneTurn
stuttle@stoneturn.com
+1 617 570 3773

Daniel Fuller
Managing Director, StoneTurn
dfuller@stoneturn.com
+1 617 570 3702

Usually, when someone tells you that the world has changed or that an industry has experienced a paradigm shift, it is safe to assume they are being hyperbolic. However, it is no exaggeration to say that the way we work has fundamentally changed. Faced with the dangers of COVID-19, vast portions of the workforce have transitioned to remote work [almost overnight], leaving businesses and their HR teams to adapt to this new reality quickly. As many states and countries consider phased plans to reopen their economies over the next few months, it's clear that companies won't return to business-as-usual anytime soon.

Nowhere is this adaptation more essential than in the area of asset management and data security, but the speed of the transition means that IT and operations teams may not have had sufficient time to update their practices. Moreover, HR departments will have to acclimatize to this new normal "on the fly" leaving them increasingly susceptible to malefactors and potential dangerous activity by current and or departing employees.

A report from the Identity Theft Research Center found that 36 percent of the roughly 1,400 data breaches reported in 2019 were due to unauthorized access that required no hacking, phishing, or other illegal activity. As workers make the jump from the office to their couches, many are relying on personal computers and devices to keep them productive. Either out of convenience or because businesses do not have enough portable devices for

all the employees now working from home, your company data is now more likely than ever to be accessed through personal devices. Whatever the case, this will create greater opportunities for confidential data to become commingled with personal files on a device that is not controlled by the business. For willful bad actors or employees who may have been laid off, the belief that their activities will not be tracked across a home network can be a compelling added incentive to copy company data for personal use.

How HR Teams Can Prevent Loss of Confidential Data

Fortunately, there are proactive steps that organizations and HR teams can take to prevent loss of confidential data and proprietary assets during the COVID-19 crisis without limiting workers' ability to do their jobs remotely:

1. Lock Down USB Ports: Being outside an office environment and physically out of sight of managers and coworkers makes it even easier to transfer company files to a portable USB drive. If your company is issuing laptop computers to employees to facilitate remote work, make sure that USB drives are locked down.

2. Implement a Data Loss Prevention System: Whether employees are working from a company owned device or their personal computers, requiring the installation of data loss prevention software to detect or prevent data breaches and unauthorized transmissions can help limit your exposure.

3. Employ a Monitoring Solution: To exfiltrate a large amount of data, a remote employee could simply transfer data from a work computer to a personal computer or download data stored on your company network or cloud repository. A monitoring solution can track which employees access these resources enabling you to audit that access against that employee's approved tasks and regular responsibilities.

How to Deal With Suspicious Employee Behavior

While prevention is critical, it may be difficult to implement many of these solutions during a prolonged crisis where time is of the essence and many employees have already scattered out of reach. In this case, forensic technology plays an essential role in detecting potential misappropriation of confidential information after the fact and securing data that may have been lost or misplaced. Savvy organizations will use forensic technology proactively. Some important practices to keep in mind if suspicious employee behavior is detected:

1. Analyze USB Device History: If you suspect a breach on a company owned device, it is prudent to review logs to see if and when USB devices were connected and if files have been exfiltrated to a USB or portable drive.

2. Review Internet History: If a data breach is suspected, review the user's internet history during that period to better understand their activity and look for signs of trouble such as accessing a personal cloud storage service or non-company email provider.

3. Study User Activity During Quarantine: In some cases it may be useful to analyze all of a user's device activity for a given period. Most businesses began transitioning employees to work remotely in March 2020. A review period should start in March and span the entire period until quarantine is lifted and workers return to the office.

4. Enable Remote Collection of Email: Review employee's corporate email activity during the quarantine period, paying special attention to any messages sent to personal accounts.

5. Enable Remote Collection of Company-Provided Smartphone Data: For employees using a company mobile device such as a smartphone or tablet, collect and review device backups during the period when a breach is suspected.

Employing forensic technology methodologies and following these basic practices can help to detect misappropriation of company breaches that may have gone unnoticed during this period of unprecedented disruption.

Trust Your Employees, But Be Proactive With Cybersecurity

For most businesses, the transition to a remote workforce will bring several challenges, and most employees will act in good faith to protect company assets during this challenging time. However, by taking proactive steps to monitor and control the flow of data, and employing forensic tools to review and understand how data moved during this period of lockdown, your HR, IT and operations teams can protect their businesses from unauthorized data exfiltration as well as from the accidental exposure of company assets.

About the Authors

Sean Tuttle, a Partner with StoneTurn, leads StoneTurn's Forensic Technology practice and brings more than 16 years of experience in managing investigations and litigation matters involving technology as a principle component.

Daniel Fuller, a Managing Director at StoneTurn, brings more than fourteen years of experience in forensic technology services, specifically in identification, preservation, extraction, documentation and analysis of electronically-stored information ("ESI").

The above article originally appeared in **Toolbox for HR July 2020**.