AVANSIC®
E-Discovery & Digital Forensics

Securing Your Firm or Business Before (And If) an Employee Betrays You

By Tom Vincent, Attorney, Gable Gotwals
Dr. Gavin W. Manes, CEO, Avansic

Introduction

Imagine that several months ago, you hired an energetic employee that originally had a lot of ideas for the growth of your company, but now just has a lot of excuses for poor performance. You can't prove it, you've heard through the grapevine that he is looking for another job with a competitor – and may be using your company's intellectual property as an incentive for a lateral move. Without any hard evidence, what do you do?

Assess and Address Your Environment

If you haven't done so already, it's time to assess how one of your most valuable assets – your company's information – flows through your company: who has access to it, how they have access to it, and what that access allows them to do. Much like the process a plumber goes through to determine how water flows through pipes in a building, including any leaks, this exercise can show you not only how effective (or not) your information security efforts may actually be, but also where information may be escaping without your knowledge.

Once you've identified how things are, take stock of your company policies, procedures, and controls to identify how you'd like them to be – and take steps to make that happen. Make sure the importance of securing information is communicated, including the penalties for failing to secure it. Where possible, supplement restrictions on information access and movement with after-the-fact monitoring and verification. Once these steps are in place, however, they won't enforce themselves.

Empower Your Employees

You may not be able to keep an eye on your questionable employee, but odds are you have employees that may be around him on a regular basis that can. All employees should be trained on your policies and procedures, including how to report suspected violations. Depending on your circumstances, you may also consider requiring annual certification by your employees that they understand and comply with your policies, and are not aware of anyone else who may have violated them (unless, of course, they are – in which case, they should report that with their annual certification).

These measures can and should be reinforced with regular discussions in departmental meetings, managerial discussions, and other employee activities. The more comfortable employees feel talking about it, the more likely they are to raise the issue – particularly when the message is, "By protecting this information, we're protecting you as well as the company."

Now imagine the difficult employee situation turned into a difficult employee *separation* situation. It was complicated and challenging but you did all the right things: changed passwords, took their devices out of service and stored them securely, changed door

codes, and did exit interviews. At the time, you had a suspicion that he may have taken some of your company's information and/or intellectual property, but it wasn't enough to act on. This week, you've learned more through the grapevine - that it's very likely he took proprietary information and he's using it at another business. So now what?

What Devices?

You want to find out what happened, but what can you realistically expect? That depends on two things: the type of electronic devices involved and how those devices were handled when the person left. Typically, at least one cell phone and one computer are involved. Other sources of information include centralized file share, email stores, and additional tablets or portable devices (i.e. iPad, laptop, second cell phone, FitBit, external drives). If devices or files haven't been used in the intervening time, there may be much more useful data available. The ideal scenario, where the most information is available, occurs when a forensics image was taken immediately after separation.

What You Could Learn

A forensic examination of mobile devices may reveal text and MMS messages, pictures, videos, call history (incoming, outgoing, missed), contacts, voicemails, calendar appointments and email, and app usage. This is not an inclusive list and some devices may include additional information. Some information can be retrieved even if it has been deleted; however, it depends on the type of collection that forensics experts are able to perform (which depends on the type of cell phone). Some information may also be available that was synced to the cloud (i.e., iCloud or iTunes accounts).

For computers and other data stores, forensic examinations typically center on file transfer activity: a client list or engineering drawing that was emailed, put on a thumb drive, burned to DVD, or uploaded to a file sharing site.

Forensics examiners can determine this type of activity through investigating file metadata, performing email and internet history analysis, performing external device analysis (i.e., when USB drives were plugged in), creating a user activity timeline, and performing an MRU (most recently used) analysis. User activity can include dates and times of document copies (especially to external media), dates and times of document deletions, websites visited, and more. Almost any type of data copying leaves a trail of breadcrumbs to be followed by forensics investigators.

What Now?

Taking a forensics image of target devices (if you haven't already) is the first critical step, followed by an investigation by a forensics examiner. Narrowing dates, user activity, and filetypes makes this process faster and less costly.

If not already involved, counsel should be engaged to address the various issues that may arise, including:

- Determination as to whether a breach reportable under state or federal law has occurred and if notification to customers is required
- Determination as to additional notification(s) that may be required to vendors, law enforcement, media, or the company's insurance carrier(s)
- Establishment of privilege as applicable to company communications

Counsel may also advise as to appropriate action to be taken against the employee and/or the employee's new employer, which can have an added effect of showing other employees your commitment to protecting the company and them.

What About Next Time?

No one can prevent someone's poor decision making, but preventive measures applied early may not only identify problem situations but put protections in place even before an employee starts. As part of your new hire process, consider having the employee certify that they understand that employer information is proprietary and is not to be misused – you may also consider including a statement that the employee has not taken information from a prior employer (to reduce the risk of the communication described above being directed at you). For certain employees, consider a more formal agreement, including non-solicitation and/or non-competition clauses to prevent the use of any such information that may be taken (although such agreements should be drafted carefully to ensure enforceability).

Case Study #1- Clandestine Cloud Storage

Several days before an employee resigned, they installed a cloud storage syncing tool on their work computer. Overnight, they uploaded email files, drawings, business plans, and other documents to the cloud. When the former employee went to their new company, they installed the same syncing tool and downloaded everything that had been previously uploaded. When the former company learned that some of their information ended up in the new company's hands, they initiated an investigation.

By examining data in the employee's cloud storage account, it was determined that the former employee opened a business plan, deleted the former company's logo, put the new company's logo in its place, made a few other edits, then saved that document to their new work computer. Since the cloud syncing program was still running on the new work computer, it synced the newly saved document back to the cloud storage system. Because of this, all investigation could take place only with access to the cloud storage system and no computers at the new company needed to be examined. A jury determined there was intentional action to take material that was then used in a business transaction and found for the former employer in the lawsuit.

Case Study #2 – Not Always What It Seems

An employee was terminated for taking documents from company computers. The former employee filed a lawsuit for wrongful termination. The IT department performed a cursory examination and reported that an external hard drive had been plugged in, documents had been copied to it, and then the hard drive was removed. Other employees reported seeing that hard drive taken home by the former employee. The company hired a forensic investigator who determined the file copy in question was made to the company's servers, not to the external hard drive. Indeed, the employee had re-used the C: drive designation, which caused confusion on the part of IT staff; this gave them the impression data was copied to the drive instead of the server. After this finding, the wrongful termination lawsuit was settled and the company updated their separation policies and procedures, including a requirement for IT and HR to confirm any suspicions in writing prior to termination.

Conclusion

An employee taking your company's information and using it elsewhere is a difficult problem no matter the circumstance. Even before you suspect anything **has** happened, it's a good idea to know how something **could** and work to prevent it. If you find out

about it after the fact, forensic investigation can help pinpoint the time, method and content of any data transfer and that information can be used both to protect the company and for legal recourse against the employee. The more information you have, the better you can mitigate damage from that transfer and prevent future transfers from occurring.

About the Authors

Tom Vincent – Banking, Compliance and Data Security/Privacy Attorney, Gable Gotwals

Tom C. Vincent II brings extensive experience in banking, financial services, and trust company compliance to his practice at Gable Gotwals. His background includes serving as The F&M Bank and Trust Company's Chief Compliance Officer, where he chaired the bank's Compliance and Ethics Committee. Tom also held several compliance-related positions with BOK Financial Corporation (BOKF) and its subsidiaries, including serving as Chief Compliance Officer for BOSC, Inc., BOKF's subsidiary broker-dealer, and also as Senior Vice President and the Manager of Corporate Governance and Wealth Management Compliance. He is a Certified Regulatory Compliance Manager and received his Juris Doctor from Washington and Lee University School of Law in 1994 and his Bachelor of Science in political science from Southern Methodist University in 1991.

Dr. Gavin W. Manes – CEO, Avansic

Dr. Gavin W. Manes is a nationally recognized expert in e-discovery and digital forensics. He is currently the CEO of Avansic, a firm that provides the legal, business, and government sectors with e-discovery, digital forensics, data preservation, and online review services. He founded Avansic in 2004 while serving as a Computer Science professor at the University of Tulsa. There he led the creation of nationally recognized research efforts in digital forensics and telecommunications security.