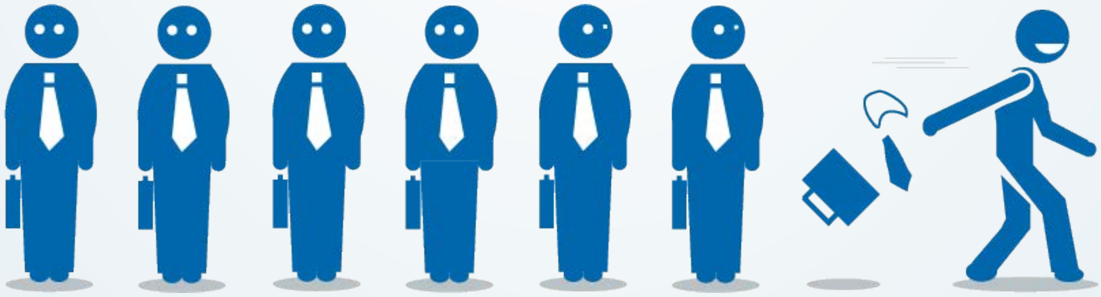
4Discovery

CASE STUDY:

EXECUTIVE STEALING COMPANY DATA



WRITTEN BY THE DIGITAL FORENSIC EXPERTS AT 4DISCOVERY

Executive Including Personal Address on Company Emails Raises Business Owner's Concerns

SMB data analytics firm / central office and remote workforce

THE ISSUE

The owner of a small data analytics firm had noticed that the organization's head of sales had included his personal Gmail address on the CC of a forwarded email. A look at previous communications from the email server revealed that this sales executive had been frequently BCC’ing their personal Gmail address in sent emails. There was a raised level of concern when the owner received notification from their email service provider, MailChimp, that a download of the company's contact records had been completed, without the owner performing this action. The owner's suspicions prompted them to contact their corporate attorney, who engaged 4Discovery to investigate the activity.

THE APPROACH

The first step was to work with the business owner and counsel to determine what platforms, files, and data the sales executive had access to. This includes the types of company-issued devices and systems that the executive accessed remotely through the Cloud. It was essential to understand the owner's hypothesis regarding the activity taken by the executive. For example, the sales executive did have access to the company's MailChimp account but had never previously downloaded the entire contact list. In addition, including a personal email address on outgoing messages was confusing, so determining when and why that was occurring was a blank that needed to be filled.

Understanding the firm's data landscape and the owner's issues helped craft a tailored approach to where to start the investigation. The first two data sources that needed to be preserved with a digital forensic image were the company's Google Workspace (formerly G Suite) account and the sales executive's company-issued laptop.

Upon analyzing the company's Google Workspace, which contains the corporate Gmail account, a manually added rule was active in the settings that included the sales executive's personal email address in the Bcc line of every email the executive sent. Looking in the Sent folder, this had been occurring for over six months. This rule covered every one of the executive's email messages, from simple transactional emails to those with attachments containing sensitive company information. A spreadsheet of these emails, including the attachment file names, was provided to the owner. The owner determined which of these attachments contained sensitive company data that shouldn't have left the organization through this information report of findings.

When analyzing the company-issued laptop, there wasn't any activity that would indicate data was being copied from the company to another destination. This included limited activity on the company laptop related to USB storage, internet browser history, downloads, and linking to the company's Google Workspace shared drives. Therefore, it was determined that the MailChimp contacts were not accessed from or downloaded to the executive's company-issued device.

Based on the finds of the Gmail forwarding rule and the lack of activity on the company laptop, the owner reached out to the executive to determine if they were using any other devices while working remotely. The owner confirmed with the executive that they had a personal device at home that they were using to conduct company business.

THE PIVOT

The business owner's legal counsel drafted a TRO and requested that the executive's personal laptop be imaged and analyzed. After that analysis, it was identified that numerous activities were taken on the executive's personal device to exfiltrate company data. This included records of the company owner's personal USB drive (which contained a backup of the owner’s computer as well as a number of personal documents and photos) being plugged into the executive's personal laptop on multiple occasions.

The USB drive was physically located in the desk of the owner at the company's office. The executive was able to take the USB when they were alone in the company office. was taken When the USB drive was plugged into the executive's personal computer, the activity logs were able to determine what specific files were accessed, copied, and transferred over to another data source location.

Working with the owner, it was determined which of these documents or actions were based around proprietary or sensitive company data and which files would need to be identified in terms of their final location and ultimately remediated.

> "The pragmatic approach was essential for a developing scenario that had more questions than answers. As the data and analysis gave us a clear picture of what was happening, we were able to craft a strategy that was in my client's best interest."

THE OUTCOME

Ultimately the business owner had a hypothesis and a blank they were trying to fill. The executive's actions were chronicled in detail based on the digital breadcrumbs left behind. The progressive approach of imaging and analyzing what was important and relevant, helped counsel adjust their legal strategy based on the digital forensics facts of the matter.

From the business owner's standpoint, they were able to protect their client's data, have it successfully remediated from all destinations data sources, terminate the executive for cause, and avoid litigation.

It's important to know that the evidence isn't always on the work-issued device(s) in trade secret matters. The exfiltration of company data is occurring at a higher rate through personal devices and accounts.

THE SOLUTION

Every trade secret matter is different and requires a custom approach. We want to hear about your unique situation and provide a unique solution to support your matter:

visit: **4discovery.com**
email: **info@4discovery.com**
phone: **312.924.5761**