Legility

Case Study

Using RGC to Collect Data from an Organization's Facilities Across the Country

Challenge

Covertly collect data from 450-plus custodians in 15 locations without physically sending any analysts to the sites.

Solution

Legility used five Remote Governance and Collection (RGC) units to image more than 450 devices to quickly respond to a government inquiry.

> **Legility collected at close to 30 TB from more than 450 custodians located in 15 offices across the country. Using RGC instead of traditional on-site collection saved the client time and money normally spent on travel.**

Overview

A government investigation required collection from a corporation's 15 different sites across the country. The data needed to be acquired from approximately 30 devices at each location without notifying the custodian. Some of the data was also encrypted, which complicated the process because decryption can take between four and eight hours per device.

Outside counsel formed three teams to travel to each facility to interview custodians and identify the records needed. As soon as each team left a facility, collection needed to begin.

Legility used a total of five RGC devices to collect from the 15 sites, shipping the devices from location to location throughout the process. Using this method instead of on-site collection allowed Legility to scale the acquisition very quickly across all of the collection sites. In total, close to 30 TB was collected, and each collection took only two to three days or less.

Installation

To install an RGC device at an office, Legility worked closely with IT staff or another representative if the site didn't have an IT person. After the device arrived on site, Legility technicians had a conference call to walk the representative through setting up the unit behind the firewall and getting it connected to the internal network.

Typically, the unit was placed in the server room or another secure office that could be locked. Once Legility verified the licensing software and that they could control it remotely, collection was ready to begin.

Counsel provided a list of computer or file share locations that needed to be collected from each facility. Legility used that list to work with corporate or local IT staff to identify the exact computer names and/or IP addresses of the targets. From there, Legility performed collection.

The speed of each collection depended on a few factors, including internal network speed and whether the computer was on wireless network or plugged in directly. Some of the facilities had a 100 MB network, which is slow by today's standards. If a custodian had a good amount of data, it could take one or two days to collect from the computer. For this reason, RGC can resume from where it left off if a computer is turned off during collection.

Each RGC device has six different hard drives inside of it. Some devices were sent back to Legility to have the hard drives changed while others were sent directly to the next facility. If an RGC device was sent directly to a new location and a drive needed to be changed, Legility would encrypt the data and then explain to the local IT staff via conference call or screen sharing how to eject it. Legility sent evidence bags to those locations so the IT staff could seal the data and send it back to Legility in a secure manner. With this functionality, Legility could begin processing while the RGC started collecting for the next location.

A few of the company devices couldn't be collected for various reasons, like the custodian being on vacation while collection took place. Toward the end of the acquisition, Legility coordinated with the local IT team to do another remote collection via remote collection portables.

Installation, cont'd

Legility mailed an encrypted hard drive to the site, which was plugged into the network by the local team. This allowed Legility to remotely run and verify collection. Then, the IT team shipped the drive back to Legility's headquarters for processing.

A lot of the custodians' data was heavily encrypted. If it had been collected on-site, decryption would have added significant time to the process. Since RGC was installed behind the company's firewall, Legility was able to preform collection as an agent of the company and did not have to decrypt the data.

Conclusion

Remote collection was critical in this case. The massive size of the investigation made some employees nervous so RGC's ability to collect behind the scene was an added benefit. The RGC platform allowed Legility to scale collection very quickly without ever putting boots on the ground at any of the facilities. RGC's installation behind the firewall was also critical to avoid hours spent decrypting data.

Legility collected at close to 30 TB of data from more than 450 custodians located in 15 offices across the country. Using RGC instead of traditional on-site collection saved the client time and money normally spent on travel. Accelerating the process was also critical in order to achieve a quick response to a huge government inquiry. While the size of this project could have been intimidating, the RGC units simplified collection to save time and money, and more importantly, fulfilled the government's inquiry as quickly as possible.

Legility Team

Our secure Data Solutions Center enables our forensic team to quickly, securely recover and examine electronically stored information (ESI). Our forensic experts maintain comprehensive chain of custody records and provide detailed reports on every action taken, ensuring the evidence produced is validated and defensible. We are also available to testify to our findings in court or through prepared affidavits.