Case **Study**

VESTIGE
Digital Investigations

CyberSecurity | **Internet Intrusion**

Scenario

Vestige was contacted by the attorney for a material handling company after their e-mail system was broken into from the Internet. While in the midst of defending a wrongful termination matter at the company, e-mail accounts for two current employees were commandeered by an Internet intruder and used to send false, but harmful evidence to a third party recipient.

> ***Had the in-house IT department even 'poked around' to see what they could find, relevent evidence unnecessarily would have been destroyed.***

Vestige's Hunt Team who specializes in intrusion detection and forensic analysis, swung into action to trace the origin of the break-in and to help identify the sender of the harmful e-mails.

Working to swiftly identify all of the relevant log files and the various points for data collection, Vestige worked with the company, it's Internet Service Provider, and a number of other ISP's to track and trace the origin. Vestige even helped in coordinating and sending subpoenas for the necessary information.

To help protect the culprit's anonymity, the suspect rented computer time at a popular national computer retail establishment. In the end, this was not enough to protect anonymity.

Vestige worked with the Information Security Department of the retail establishment to obtain the surveillance video footage that showed indisputable evidence of who the culprit was. The rest, as they say, is history.

Key **Points**

- Client hired Vestige immediately, helping to ensure that volatile information used to track the culprit remained available .
- Vestige proved the e-mails were the result of a break-in and not to be treated as evidence against the company
- Identity of culprit traced to the physical retail establishment used to "anonymously" send the e-mails
- Culprit admits break-in

Success

Beyond hiring the right people for the job, our client set themselves up for success by hiring a specialist as soon as they realized they had a problem. Setting egos aside, the in-house IT staff realized that in order to ensure the admissibility of the findings, they would need to rely on a company that understands electronic evidence and the procedures and techniques needed to protect the integrity of the evidence. While the IT department was very capable of running the day-to-day operations of the company's IT environment, management realized anything less than a professional job surrounding the handling of the evidence might end up being even more detrimental in their case. In this incident, simply "poking around" to see what they could find would have destroyed crucial evidence that was used to ultimately prove who the culprit was.

Contact Vestige today to discuss your CyberSecurity needs.

TURNING DIGITAL EVIDENCE INTO INTELLIGENCE™

23 Public Square | Suite 250 | Medina, Ohio 44256 | **800.314.4357** | www.VestigeLtd.com