**Investigative Report on ACE Data Breach**

Nwachukwu Edumanichukwu

Bellevue University

CYBR420-308H Cyber Investigations & Forensics

Professor Anthony Geron Tony

March 5, 2023

Case number: 00747

Firm: ACE Consulting

Date of Incident: March 5, 2023

Incident: Data Breach

Chief Investigator: Nwachukwu Edumanichukwu

***Introduction:***

ACE Consulting, a consulting firm with approximately 500 employees in six southern US cities, has been experiencing a series of data leaks. The clients' proprietary information and research and development have shown up in competitors' hands, and employees have reported unusual activities in personal accounts and personal email. The company has hired an independent investigator to investigate some company-owned computers and devices to determine if there is an insider in the company.

This report summarizes the findings of the investigation into two primary targets: James Brown, a project manager who has worked at the main office for ten years, and Sam Abrams, a new member of the IT support team. The report analyzes both targets' computers, devices, and online activities to determine if there is an insider threat in the company.

***Executive Summary:***

This investigative report is about the potential insider threat at ACE Consulting, a company that provides consulting services in six cities in the southern United States. Several clients have reported that their proprietary information and research and development have shown up in competitors' hands. Moreover, some employees have noticed unusual activities in personal accounts and personal email. James Brown, a project manager who has worked at the main office for ten years, and Sam Abrams, a new member on the IT support team, are the primary targets of this investigation. The report includes a detailed analysis of both targets' computers, devices, and online activities to determine if there is an insider in the company.

The investigation found that James Brown was using a Dell Latitude 3793 Core i7 M640 laptop with a 500GB HDD running on Windows 10 Professional 64-bit. He had a SanDisk 8GB USB flash drive and several data DVDs on his desk, along with a personal Gmail account that he accessed regularly from his laptop. Upon reviewing the PC's hard drive, the investigation discovered that there was a hidden drive/partition since VeraCrypt was installed.

Sam Abrams used a Dell OptiPlex 760 with an Intel Core 2 Duo CPU E8400, 8GB, 500GB HDD, DVDRW, running on Windows 10 Professional 64-bit. He had a corporate email account and a Yahoo account, which he accessed from his PC. From his browser history, it was observed that he uses Facebook, Craigslist, and Dropbox.

Based on the investigation's findings, it was concluded that James Brown was likely the source of the information leaks. The VeraCrypt installation and the presence of a hidden drive/partition suggest that he was deliberately hiding data. Additionally, his personal Gmail account usage on the company laptop raises questions about his motives. The investigation did not find any evidence of wrongdoing by Sam Abrams.

The report recommends that the company takes immediate action to prevent any further data leaks, such as revoking James Brown's access to company systems and conducting a thorough review of all the data he had access to. The company should also update their cybersecurity protocols and provide cybersecurity training to all employees to prevent future incidents.

***Jurisdictional Issues:***

There are no jurisdictional issues between the six locations as they are all within the same region and governed by the same laws and regulations. However, since the investigation is limited to company-owned devices of two primary targets, and they’re located in the main office. This is not a significant issue for this case.

***Background Synopsis:***

ACE Consulting has a mix of Microsoft and Linux servers and PCs with several Mac computers used for various consulting activities. The company uses Active Directory, an Apache Web Server for the Internet web site, four servers used as file storage (one in each office), four servers housing applications used for consulting activities, a training server, five MS SQL database servers, and Office 365 for email. System updates and patches are run from the main office, but some systems and third-party products are not kept up to date. Each satellite office has 3-4 servers for storing files and running local applications. Each office has its own decentralized wireless network connected to the production network. Employees work remotely and use their login and password to gain access to the corporate systems. James Brown has a Dell Latitude 3793 Core i7 M640, 16GB, 500GB HDD, Windows 10 Professional 64-bit, and is suspected of having a hidden drive/partition since it has VeraCrypt installed. Sam Abrams has a Dell OptiPlex 760 – Intel® Core 2 Duo CPU E8400, 8GB, 500GB HDD, DVDRW, Windows 10 Professional 64-bit, and has been found to have personal email accounts, including Yahoo and Facebook, and uses Dropbox.

***Investigation Plan:***

The investigation will be carried out by examining the computer systems used by James Brown and Sam Abrams. The investigation will begin by creating forensic images of their computers to ensure the preservation of data integrity. The images will be analyzed using a combination of automated and manual techniques to identify any suspicious activity or files. The investigation will also involve interviewing employees who work closely with James Brown and Sam Abrams to determine if they have any knowledge of their activities. The investigation will be conducted discreetly to avoid any disruption to the company's operations.

In the case of James Brown, the investigation will focus on his personal computer, the SanDisk 8GB USB flash drive found on his desk, and the data DVDs. The hidden drive/partition suspected to be present on his computer will be investigated thoroughly. The investigation will also examine his Google mail account and Google Drive to determine if any sensitive data has been stored or transferred.

In the case of Sam Abrams, the investigation will focus on his use of personal email accounts, Facebook, and Dropbox. The investigation will also examine his computer for any suspicious activity or files. Interviews with employees who have worked with him closely will be conducted to determine if they have any knowledge of his activities.

All servers hosting critical company data, including file servers, email servers, and database servers, would need to be analyzed. Information such as logs, access control lists, and system files could be examined for evidence of unauthorized access or data exfiltration. Network traffic logs could be analyzed to identify any unusual or suspicious network activity, such as unauthorized access attempts or data transfers.

***The tools needed for this investigation would include:***

***Hardware Tools:***

***Write-blocker:*** This tool is used to prevent any modifications to the original data during the investigation process.

***Forensic workstation:*** A computer system dedicated to forensic investigations, which must meet specific hardware and software requirements to ensure the integrity of the data.

***External hard drive:*** Used to store the acquired data during the investigation.

***Software Tools:***

***Forensic imaging software:*** Encase Forensic Imager, to create a forensic clone or bit-for-bit copy of the hard drives and storage devices without altering the original data (EnCase Forensic Suite, n.d.).

***Data recovery software:*** Recuva, to recover deleted or lost files and data from the hard drives and storage devices (Recuva, n.d.).

***Forensic analysis software:*** Encase Forensic, to analyze the forensic images and extract relevant information such as email logs, browser history, and system logs (Digital Investigations and Forensics, n.d.).  
***Password cracking software:*** John the Ripper, HashCat and Cain and Abel, to attempt to recover passwords for encrypted files and archives.

***Network analysis software:*** Wireshark, to analyze network traffic and identify any suspicious activities (Wireshark, n.d.).

***Email recovery and analysis software:*** Forensic Email Collector and Email Examiner, to recover and analyze email messages and attachments.

***File hashing software:*** QuickHash and HashMyFiles, to generate and verify hashes of the evidence to ensure the integrity and authenticity of the data.

***Evidence List:***

**James Brown's Desktop Computer**

a. Make: Dell

b. Model: OptiPlex 9020

c. Serial Number: AB123456

d. Removable Media: None

e. Operating System: Windows 10

f. Installed Applications: Microsoft Office 365, Chrome Browser, Slack, Adobe Acrobat

g. Other identifying information: Asset tag number JBR-001

**James Brown's Laptop Computer**

a. Make: Lenovo

b. Model: ThinkPad T480

c. Serial Number: CD123456

d. Removable Media: 1x USB Drive (Brand: SanDisk)

e. Operating System: Windows 10

f. Installed Applications: Microsoft Office 365, Firefox Browser, Dropbox, Cisco AnyConnect

g. Other identifying information: Asset tag number JBL-001

**Sam Abrams' Desktop Computer**

a. Make: HP

b. Model: EliteDesk 800 G5

c. Serial Number: EF123456

d. Removable Media: None

e. Operating System: Windows 10

f. Installed Applications: Microsoft Office 365, Chrome Browser, Cisco AnyConnect, Slack

g. Other identifying information: Asset tag number SAD-001

**Sam Abrams' Laptop Computer**

a. Make: Dell

b. Model: Latitude 7490

c. Serial Number: GH123456

d. Removable Media: None

e. Operating System: Windows 10

f. Installed Applications: Microsoft Office 365, Firefox Browser, Cisco AnyConnect, Adobe Creative Cloud

g. Other identifying information: Asset tag number SAL-001

**ACE Consulting Server 1**

a. Make: Dell

b. Model: PowerEdge R740

c. Serial Number: XYZ123456

d. Removable Media: None

e. Operating System: Windows Server 2016

f. Installed Applications: Microsoft SQL Server, IIS, Active Directory, McAfee Endpoint Security

g. Other identifying information: IP Address 192.168.1.100, Hostname ACEServer1

**ACE Consulting Server 2**

a. Make: HP

b. Model: ProLiant DL380 Gen10

c. Serial Number: ABC123456

d. Removable Media: None

e. Operating System: Windows Server 2019

f. Installed Applications: Microsoft Exchange Server, VMware vSphere, Symantec Endpoint Protection

g. Other identifying information: IP Address 192.168.1.101, Hostname ACEServer2

**Network Switch**

a. Make: Cisco

b. Model: Catalyst 3650

c. Serial Number: DEF123456

d. Removable Media: None

e. Operating System: Cisco IOS

f. Installed Applications: N/A

g. Other identifying information: IP Address 192.168.1.1, Hostname ACESwitch1

**Router**

a. Make: Juniper

b. Model: SRX240

c. Serial Number: GHI123456

d. Removable Media: None

e. Operating System: Jun OS

f. Installed Applications: N/A

g. Other identifying information: IP Address 192.168.1.254, Hostname ACERouter1

**USB Drive (Belonging to James Brown)**

a. Make: SanDisk

b. Model: Ultra Flair USB 3.0

c. Serial Number: JK123456

d. Capacity: 64 GB

e. Other identifying information: Labeled "JB-Confidential."

***Recommendations:***

***I would recommend the company to take these following steps to stay proactive:***

1. Implement a strict policy that prohibits the use of personal email accounts and external storage devices for work purposes.

2. Implement a strict patch management policy to ensure that all systems are up to date with the latest security patches and updates.

3. Implement a strict password management policy to ensure that employees are not sharing passwords and are using strong passwords.

4. Implement a strict access control policy to ensure that employees only have access to the systems and data that they require to perform their duties.

5. Conduct regular training for employees on the importance of information security and the risks associated with data breaches.

6. Monitor employee activity on company-owned devices to detect any suspicious activity and take immediate action if any is detected.

7. Conduct regular audits of the IT infrastructure to identify vulnerabilities and take action to mitigate them.

**References**

Information provided in this case study.  
*Digital Investigations and Forensics*. (n.d.). Retrieved from OpenText EnCase Forensic: https://www.opentext.com/products/encase-forensic

*EnCase Forensic Suite*. (n.d.). Retrieved from https://e-forensic.ca/products/encase-forensic-suite/

*Recuva*. (n.d.). Retrieved from https://www.ccleaner.com/recuva

*Wireshark*. (n.d.). Retrieved from https://www.wireshark.org