Bellevue University Cybersecurity Program

J&L Coffee Inc. Case Study

Instructions: Below are details about a fictitious business requiring improvements to its security. You have been hired as a security consultant for this business. Use the details from this case study according to the directions found in the various module's assignments.

During your initial engagement with J&L Coffee you given an overview of your task by President of J&L Coffee Inc., Sandy Scott, who hired you for this engagement.

Transcript of interview with Sandy Scott, President of J&L Coffee.

Welcome! I'm Sandy Scott, the president of J&L Coffee Inc. Recently, our company suffered a security breach where hackers obtained credit card data on over 25,000 of our customers. I need your expertise to ensure this doesn't happen again. Come on, let's get started. First, I'll give you a little background about our company and then I will go into detail about the security we currently have in place.

J&L Coffee Inc. is a coffee shop franchise that supports over 100 coffee shops located in New York, New Jersey, Delaware, and Pennsylvania. Jim and Loretta Pierce started the original J&L Coffee coffee shop at a railroad passenger station back in 1954. Since then, their children and grandchildren have transformed the company from a single coffee shop into a chain of coffee shops, and, most recently, into a publicly traded franchise business. The franchise business provides shop owners with everything they need to open and run their own operation, including fixtures, restaurant products, support services, coffee and food. As another service to franchise owners, we resell credit card payment processing services to them at competitive rates. J&L Coffee reimburses, up front, for credit card transactions that are funneled through their payment processing system as an incentive for franchise owners to use our services.

As for location of the corporate headquarters, J&L Coffee Inc. calls Windsor, Pennsylvania home. Both the corporate headquarters and principle warehouse are located there. We built the campus from the ground up at that location because it was central to our operation and both the business climate and tax structure were favorable. The campus currently employs slightly over 400 people that see to the day to day business operations.

The campus' physical security system includes a perimeter fence, cameras, smart card access points, alarms, and a full-time security staff.

The campus also features a three-layer wired network infrastructure. Plus, it has full wireless access provided by an Aruba Networks grid. Comcast Business Solutions provides J&L Coffee with Internet. We have a number of security appliances and devices already in place, but I'm not sure how effective they are. As for the active directory domain, there is a single one for the entire campus. It was configured using default settings, and uses the default domain group policy with one exception. Password history and complexity requirements have been disabled to make it easier for employees to use passwords they can remember and reuse them if they want. The rationale for making this change was that I had difficulty remembering my password, so I began to write it down. A member of the cleaning crew saw it and used my machine to view pornographic material. When I discovered the breach, I fired the person responsible and directed the password policy change.

Our headquarters also features servers, and web hosting; however, the specifics for each are a bit detailed. I'll have my chief of IT send you a summary. Next, let's focus on the on and off campus workstations.

The company has over 400 Dell Optiplex 3080 workstations on campus. Each computer is installed with Windows 10. Plus, all computers are joined to the company's Active Directory domain. Off campus, the default configuration for new coffee shops consists of a high speed Internet connection supplied by a local provider, a Network Address Translation firewall device that includes a wireless access point, an office computer, and two point-of-sale computer systems from Clover that includes credit card processing software. Even though we try to stay up-to-date with the latest software and hardware, our system is not immune to failure. While all employees have user names and passwords for the system, there have been problems with computers becoming infected with malware because the point-of-sale software can be minimized and the host computer used for web browsing.

Now that I've explained the history and background of my company as well as the infrastructure of our system, it's time to get to work.

IT & Security Infrastructure Summary provided by J&L Coffee chief of IT

Below are details on the Information Technology and Security infrastructure, policies, and equipment currently in place at the client, J&L Coffee.

Physical security:

The campus physical security features include a perimeter fence, cameras, smart card access points, alarms, and a full-time security staff. Access to all buildings on campus is restricted through smart cards. The server room is a 1600 square foot room within the main headquarters building. It has climate control, redundant uninterruptable power supplies (UPS), and a generator with enough capacity for 36 hours of uninterrupted operation. The interior of the room is equipped with fire, water, and motion sensors, as well as cameras. The sensor and video feeds from the campus are centrally monitored by a staff of three people 24 hours a day, seven days a week.
(NOTE: Although physical security is critical to an organization's overall security posture assessment of, or modifications to, J&L physical security is outside the scope of this assignment.)

Wired network Infrastructure:

The wired network infrastructure consists of three layers. The innermost layer consists of two Cisco Nexus 7000 switches running NX-OS Release 7.3. These switches provide fully redundant 10Gbit connectivity between servers, to the Internet, and to the second layer. The second layer consists of a 10 Gbit dual fiber ring that provides connectivity between the core network and 2 Cisco Catalyst 9300 Series Access Switches located in each building on campus. The third layer consists of Gigabit copper local area networks that connect computers and Power over Ethernet (PoE) phones with Cisco 9200 PoE switches that are located in communication closets in close proximity to their users. Each subnet in the third layer is connected to the second layer through both Cisco Catalyst 9300Series Access Switches that provide access to the fiber ring for the building. Layers 1 and 2 are fully redundant. Layer 3 doesn't provide redundant connections, but less than 50% of the available ports are used on each switch. The communication closets are equipped with patch panels that would permit network administrators to manually bypass a

defective switch.

Wireless connectivity on the campus:

The campus has full wireless access provided by an Aruba Networks grid. There are two Aruba 7000 Mobility Controllers serving over 100 Aruba Networks AP-300 Series wireless access points. The wireless network interfaces directly with the corporate headquarters wired network. The mobility controller has the ability to serve as a firewall, but the default settings currently allow all traffic in both directions. In addition, the president of the company has directed that the current wireless system be configured to provide open access without logon capability because she wants to make it as easy as possible for employees to use their mobile devices. When asked about potential security issues, she said that the convenience of mobile devices outweighs the risk. She is emphatically supporting BYOD throughout the company. She had her physical security consultant walk the perimeter with a mobile device to confirm that the signals from wireless devices on the campus were too weak to register.

Internet:

The Internet connection for the company is provided by Comcast Business Services. Comcast provides a fully redundant connection to the campus.

Security appliances:

The campus network has two Palo Alto PA-5220 Firewall Security Appliances that connect the Comcast Internet connections to the core network. These two devices are currently configured to allow all traffic in both directions. These devices are capable of up to 1000 VPN connections each. However, the company chooses to forward VPN traffic through the firewalls and handle it using a Microsoft PPTP solution.

The campus also has two Proofpoint Email Protection appliances. These devices are located on the core network, and all mail traffic is forwarded through them. However, the company has not activated the subscription that updates the signature files, and some users are complaining about excessive SPAM. Other users (especially Sales and Accounts) are complaining about missing email.

Active Directory Domain:

There is a single Active Directory domain for the entire campus with two Domain Controllers running on Windows Server 2016. It was configured using default settings and uses the default domain group policy with one exception: password history and complexity requirements have been disabled to make it easier for employees to use passwords they can remember and reuse them if they want. The rationale for making this change was that our president had difficulty remembering her password, so she began writing it down. A member of the cleaning crew saw it

and used her machine to view pornographic material. When she discovered the breach, she fired the person responsible and directed the password policy change. There are five members of the IT group with domain administrative privileges.

There is a second AD Organization Unit set by the Chief Financial Officer for the Accounting and Finance Group. In this OU, all administrative assistants are also administrators in order to quickly add or remove user accounts. This OU has full password complexity turned on.

Servers:

The headquarters has a 200TByte HPE Storage solution providing a Storage Area Network (SAN) that provides storage for 10 Hewlett Packard ProLiant DL180 servers. The firmware and drivers were last updated in July 2018. The HP servers are running VMware vSphere Hypervisor (ESXi) version 6.7 GA. On that virtual platform, the company currently hosts redundant virtual servers for their domain controllers, Inventory Tracking System (ITS) Point of Sale (POS) system (Clover), accounting system, payment processing system, email system, Web site with database support for active content, Windows Routing and Remote Access Server (used for VPN connections,) authentication services, and database management systems. All virtual machines are running Microsoft Windows Server 2016 Datacenter edition. The administrative staff elected to not install antivirus software on any of the virtual servers, as that would slow them down. After all, Web browsers are disabled on all servers and by policy administrators are not allowed direct access or email.

The Web servers (IIS) and Email servers (Microsoft Exchange Server 2016 CU10) have two network connections: an internal one and external one with a public IP address. There are no firewalls on the external connections. The Web Server uses TLS 1.2 for any sensitive pages along with certificates signed by Verisign. Web developers move web pages to the Web server using File Transfer Protocol (FTP). FTP is enabled for both internal and external networks, as some programmers access the Web server from home. Security is enabled, so they must log in using their Active Directory user accounts. In addition, the system administrators have discovered that FTP is a convenient way to move files, and they often log in using their accounts, as well. Using the FTP server as a staging server, it is possible to move files from the outside to the Web server, and then from the Web server to a workstation.

Web hosting:

The Web server is used to host the company's web site. The site has two parts that are both hosted on the same server, a public part that is available over the Internet using the company's URL http://www.jlcoffee.com/ , and a "private" part that is available on the internal network only that is accessible only by using the internal URL http://www.jlcoffee.local/
Employees can log into the "private" Web site using their Windows login credentials and view their pay statements, work performance reports, vacation time, and other personal information.

The franchise owner in Scranton, PA purchased and uses the domain www.JandLScranton.com for customers at his three restaurants. He also has an active Facebook page and Twitter and Instagram accounts. He often runs contest using these sites.

Campus workstations:

The company has over 400 Dell Optiplex 3080 workstations with Windows 10 Professional installed. All computers are joined to the company's Active Directory domain. These computers are configured for IPv4 only, and IPSec is disabled by group policy. All workstations have Symantec Endpoint Protection installed. About 1/3 of employees have local administrator access in order to install and run applications. The company uses WSUS to update Microsoft applications. There is no standard process for updating other programs.

In spite of the new relaxed password rules, some employees still write their passwords down, and they can be found taped to the inside of drawers, on the bottom of mouse pads, or on notes stuck to their monitors. The company uses a Web front end for all of its applications, and the workstations are capable of accessing them using Edge, Chrome, or Firefox browsers although some internal applications still require the use of Microsoft's Internet Explorer. Remote users have access to the same applications via the VPN.

Off campus:

The default configuration for new restaurants consists of a high speed Internet connection supplied by a local provider, a Network Address Translation (NAT) firewall device that includes a wireless access point, an office computer, and two point-of-sale computer systems that include credit card processing software. The WAP router at each store is procured and set-up by the franchise owner. All franchises are supposed to have free Internet WiFi for customers. All computers are Microsoft Windows 10 machines with Norton Antivirus software. All employees have user names and passwords for the system. There have been problems with computers becoming infected with malware because the point-of-sale software can be minimized. Point-of-sale computers connect with the corporate headquarters for payment processing using Microsoft PPTP VPN clients on each machine.

Payment Processing

Our payment processing is done by Clover (https://www.clover.com/) in their cloud. Clover is PCI certified (PA-DSS) and manages our payment processing from the POS to the bank. Connections to the Clover systems go through our internet connection to Clover's servers.