Print

Mega-Corp Case Study

Mega-Corp is a multinational conglomerate consisting of two core companies. The companies are:

- Not As Tasty Health Foods—corporate headquarters, warehouse, and distribution center in San Francisco, California; and an additional distribution center in Napa Valley, California.
- Tasty Fried Foods—corporate headquarters and two restaurants in Atlanta, Georgia; three restaurants in Charlotte, South Carolina; and two restaurants in Nashville, Tennessee.

Both Mega-Corp companies are administered by a set of distinct managers, including a CIO for each organization. Each reports to the same board of directors. The organization has not had an acquisition or merger in over ten years. The product lines are stable; however profits are down in all sectors over the past two years.

IT Projects and Security

IT projects for Mega-Corp are proposed, funded, and implemented for each organization independently and are not a part of the oversight duties of the corporate board. Each organization has an IT steering committee that evaluates and funds all IT projects. This includes industry-specific systems as well as transactional systems such as HR and payroll.

Mega-Corp has assigned responsibility for security to the network administrator of each organization.

Not As Tasty Health Foods

Not As Tasty Health Foods has chosen Linux-based systems, which they maintain and operate using in-house talent. They currently manage two Linux servers used as file servers, a single server for mail and one server for administrative activities. The servers are connected to a Cat6 backbone running 100mb Ethernet through two core switches. There is no redundancy or failover capabilities set up on any of the servers. Hosts are running 10mb Ethernet between secondary switches and the desktop.

There are 65 hosts on the network that engage in a variety of activities from purchasing to personnel. The servers are housed in a closet in the basement of the facility where there are no barriers to entry for any of the staff and no environmental controls installed. The basement area is locked at night by security staff and anyone requesting access to the area must go to the guard for access to the key. Several times a year the area has experienced flooding, which has required that the equipment be placed on top of tables.

The network administrator for Not As Tasty Health Foods has chosen to protect the hosts rather than creating a hardened border between the organization and the Internet. The host protection they have implemented is the freeware version of Zone Alarm on each host along with the free version of Avast for antivirus protection. They have created an administrator account, which is shared among all of the IT staff, and simple user accounts for everyone else in the organization to use. Currently, there is a share restricted to HR staff where personnel data is stored. All other data is accessible by anyone in the organization.

Not As Tasty Health Foods has chosen not to implement mail scanning or filtering, which they view as censorship and unnecessary overhead since most attacks are pointed at Windows. Users are cautioned to be careful about opening up e-mail attachments. There are no information security policies, which are viewed as confining and having a negative impact on the creativity of staff.

Tasty Fried Foods

Tasty Fried Foods has outsourced their IT projects and network management responsibilities to Berbee Consulting and has no in-house staff managing their information assets other than the CIO, a network administrator, and four support staff.

Berbee Consulting has implemented a large Windows 2012 fileserver cluster with eight processors connected to a SAN. They have begun working with existing staff to develop information security policies that do not currently exist. The cluster and two domain servers are isolated in an administrative VLAN to which only Berbee Consulting staff has access. The entire network is set up using single mode fiber, including the connection between the host and the routers. A single core switch connects to a variety of routers to which the desktops are connected directly. The servers and core switch are housed in an environmentally-controlled computing facility. The routers are located in several locked closets that do not have environmental controls and for which the keys are widely available.

Berbee Consulting has placed an additional domain server in each of the remote locations, set to replicate every 90 minutes. Each site has a pair of Checkpoint firewalls configured to be fully redundant and also function as a VPN connection when necessary. Berbee Consulting staff control the configuration and management of the firewall and VPN. They currently save and store logs; however management of Tasty Fried Foods has requested that they not be forwarded to their existing IT staff because they do not have time to deal with them.

There are 40 hosts on the Tasty Fried Foods network. The hosts are a mixture of Win8, and Windows XP operating systems. Authentication occurs by completing a request form for access, which is sent to the Berbee Consulting staff who assigns access based on the individual job responsibilities. No groups have been activated nor has any group policy been applied to user accounts or work stations. Frequently, the request for access is delayed and staff works around it by sharing access until an account is available for the new person.

Your Role at Mega-Corp

Mega-Corp has recently hired you as their Chief Information Security Officer (CISO). You are responsible for the traditional information security areas and are also charged with providing leadership for the enterprise security staff (guns, gates, and guards).

You have been tasked with the following duties:

- Develop a framework to design and build a central data center.
- Evaluate existing biometric products and make a recommendation to the board as to how biometrics will fit with the authentication strategy for the organization.
- Develop an enterprise-level security awareness program that meets regulatory requirements.
- Recommend procedures to support coordinated effort between IT and information security which will support the security lifecycle and secure configuration of network devices.
- Create an executive guidance document related to information security and privacy regulations that impact Mega-Corp.