Print

Case Study: Global Widgets Inc.

Scenario

With high-visibility breaches in the news impacting such well-known companies as Target and Sony, the board of directors of Global Widgets has directed the CEO to ensure they are prepared to meet any potential challenges. The CEO has requested that the CIO and his technology team explore moving the entire existing IT infrastructure to a cloud-based solution. As a member of the IT team, you will be asked to provide insights into the existing environment, as well as recommendations that will result in an improved infrastructure based on the move to a cloud-based solution.

Deliverables for this case study are found in assessments 1, 3, 4, and 5.

Company Background

Global Widgets Inc. is a multinational conglomerate. The sales and distribution operations are located within the corporate headquarters in Phoenix, Arizona. Sales and solutions support staff are housed in offices within the nine sales, warehousing, and distribution centers worldwide. Global Widgets provides public wireless access for all of the guests that visit the sales and support sites.

Global Widget owns a large office complex in Phoenix where it is the sole tenant. The building houses the majority of IT staff and assets, both of which are located in the basement of the building in a secure, environmentally-controlled space. An exception is first-level support, which is outsourced to India and shares space with the sales and warehousing functions in the country.

Remote sales, warehousing, and distribution centers are all located in commercial-space settings within shopping malls. They are spaces with separate entrances and exits that have common walls with the neighboring businesses. Some of the locations have a common basement or attic space that they share as storage space with the existing businesses in the mall. These locations will include your backbone network devices (routers, switches), domain controllers, DNS, mail servers, and firewall and intrusion detection systems that allow users to work locally in the event of a broader system failure. Data on the servers is replicated twice a day from your local sites to the global locations to ensure safe and secure date transactions between sites and help with a speedy data recovery in times of disasters.

The network is segmented into 10 global virtual LANs that logically separate into the following user groups:

- Information Technology.
- Management.
- Finance.
- Human Resources.
- Marketing and Sales.
- Product Development.
- Training.
- Remote Users.
- Security and Facilities Departments.
- All other users.

New system user requests are completed by the site manager via an electronic form located on the company intranet. User management staff completes those requests from their headquarters location and they e-mail the site manager with the account and password information. Account ID is the first initial and last name of the employee. Multiples are mitigated through the addition of a 1, a 2, or, if necessary, a 3 (and so on) on the end of the ID. The temporary password is to repeat the account ID and then require the user to change the password at logon. All users

are hosted in the main Active Directory servers, which are designated as the corporate domain system for all hosts in the company.

Locations

- Headquarters: Phoenix, Arizona.
- Distribution sites: A total of three sites: New York, San Francisco, and New Orleans.
- Globally, the organization includes six locations: Germany, India, China, Australia, South Africa, and Dubai.

Employees

- Phoenix, Arizona (about 1,200 users).
- Distribution sites: New York (45 users), San Francisco (30 users), and New Orleans (25 users).
- Global locations: Germany (15 users), India (12 users), China (10 users), Australia (8 users), South Africa (6 users), and Dubai (5 users).

Main Infrastructure Items

- Hosts are primarily Windows 8, but there are examples of both Macintosh- and Linux-based systems that have been approved for use at some sites.
- Cisco routers and switches: Each site includes their local routers and switches, connected directly to the main data center located at the main headquarters in Arizona.
- Firewalls: The headquarters and distribution sites have redundant ASA firewalls at the edge of their networks, and the global locations rely on the host-based Windows firewalls to protect their systems.
- Intrusion detection: The malware solution for the organization is purchased and managed by each location and is the only form of IDS that is currently in place.
- Domain servers running Windows 2008.
- DNS servers.
- DHCP servers.
- Active Directory.
- Exchange mail servers.
- File and print servers.
- ERP system (such as PeopleSoft).

[End of Case Study]