Computer Science CSC 570 Threat Management and Disaster Recovery

Allan C Roth, PhD CISSP

Sample assignments and Projects

1. Risk Assessment Exercise

I would like you to attempt a complete Risk Assessment for a fictional enterprise. This analysis, of course, will require you to make lots of assumptions and guesses which need to be noted and documented in your paper. I want to limit your analysis to threats to the servers located in a centralized server room to keep the scope limited and Threats to connectivity to the WAN clients. You will not analyze any threats to individual workstations and desktops. What follows is a description of the server room and connectivity of those servers.

This "made-up" Enterprise is a medical practice with an Electronic Medical Record that we will call "Medco".

This EMR is needed on a 24 hour basis as this is a cardiology specialty and is used in clinic rooms AND importantly, it is used by emergency physicians in the local trauma center for treatment of patients suffering from life threatening heart issues.

The Environment

Servers

        Server 1 is Microsoft Exchange Server

        Server 2 is Domain Controller

        Server 3 is a Citrix Server (delivering applications as Thin Clients to desktops)

        Server 4 is Web Server running IIS to present main application as web pages

        Server 5 is a Server Running Microsoft SQL Server with patient data

The Servers are connected to the LAN using routers and switches.

The Servers are connected to the Internet using a single Firewall via a single connection to a single Internet Service Provider (ISP).

The Servers do connect to a WAN using this Internet connection using a VPN and the nodes on this WAN (clinics around the state) each have a single connection to an ISP in their local area.

Physically all the Servers are in a single unlocked room that has no fire suppression equipment other than the typical building sprinkler system and there are two sprinkler systems in the server room.

The servers are connected to a trunk electrical line that is not part of the medical centers emergency power system and there is no line conditioning.

The server room relies on the existing building HVAC system with heat exchangers located on the roof of the building.

The Assignment

Using the NIST Special Publication 800-30, complete a Risk Assessment to identify potential threats for which a matching vulnerability exists in the above described environment. You can pretend that you are the Security officer in charge of this

Assessment and also for your control recommendation you can make decisions from your Risk Matrix as if you were upper management.
Your paper should be at least 4 pages and should be no more than 7 pages not including items such as interview forms or spreadsheets.

2. Final Paper

Submit a final paper on a topic related to Disaster Recovery and Business Continuity. It should include an Introduction, Literature Review (with references cited), and Discussion of the Topic or Methodology, Conclusion. This paper should be a minimum of 4 pages in length and a maximum of 8 pages. You can choose your own Disaster Recovery topic or pick one of the following 3 examples:

1.Review and critique of a company's recovery from an IT disaster. Give the time line of the disaster and the recovery, the outcome and cost of this recovery, and a critique of the preparedness for this disaster with suggested improvements

2.Describe alternatives to Hot Site contracting to ensure quick IT recovery from a disaster (e.g. distributed computing and server farms, distributed data mirroring, virtualization of server farms)

3. IT outsourcing as a way of avoiding Business Continuity costs (Are there hidden costs and dangers?)

Course Documents and Links from Blackboard --Snapshot