Project

Overview

An information security review of an existing business or organization will be performed by you and the rest of the group. My hope is that you and your group will be able to identify a business of convenience to you fairly quickly. You will also need to receive approval from the business, of course.

Obviously, this assignment will not be on the order of a full-fledged technology audit that can take months to complete and usually requires technology for testing and full access to the network infrastructure. This will be more along the lines of a general control review, and information will be gathered using less technical means, such as observation, inquiry, and possible inspection (if allowed). We are also not in a position to make security recommendations.

In addition to a couple of midterm deliverables, you will prepare a white paper and a presentation detailing policies, procedures, risk assessment, preventative hardware/software, etc. that will be given at a yet-to-be-determined time around the final week of the course. Links to the deliverable details can be found below and also under the Assignments menu option.

First Deliverable (due January 30)

Second Deliverable (due February 27)

Deliverable 1

Identify the organization being reviewed. A brief description should be included. This should include information about the following

- Name of the organization (to be withheld later)
- Location
- Size and scope
- Industry type, main products and services offered
- Number of employees
- Anything relevant about the types of facilities
- If you have a point of contact already (or a probable contact), describe that

You should also include discussion about why this is an organization worthy of reviewing. Although it may be speculation at this point, what types of information assets would the organization need to protect? Do you consider them a prime target for security breaches? Any apparent vulnerabilities, either man-made or natural? *Generally speaking, if someone were to ask you, "Why review this organization?", how would you respond?* That should help produce the discussion here.

NOTE: All you have to do is describe the organization in the manner described above. There is no need to thoroughly interview anyone at this point. If you would like to provide your point of contact (or the person who would grant your group permission to perform the review) some idea of what you might be asking about, please see the 2nd deliverable description on the website. Again, for the first deliverable, merely describe the organization and justify your selection.

Reasonable expectation: around 2-3 pages

Deliverable 2

In this deliverable, you should prepare an initial draft of questions that you will use in your interview(s) with your point(s) of contact. This list should include both questions that will meet the generic guidelines of the review (see below) and questions that are specific for the organization of interest. You should treat these as sort of icebreaker questions; you are by no means limited to these questions during the interview.

Section 1 of your milestone report should include a series of generic questions that could be used within pretty much every organizational setting. Questions should involve the following:

1. General information about the organization's IS infrastructure
    1. Number & type of network users (customers, suppliers, etc.)
    2. Key information assets
    3. In-house IT support, or outsourced?
    4. Type of networks (LAN, WAN, etc.)
    5. Types of communicative media and devices accommodated (wireless, Bluetooth, RFID, etc.)
2. Security Policies and Procedures (Key policies and programs already in place)
    1. Pay particular attention to how security policies are implemented. Is management involved, as in identifying key assets, best practices, etc?
    2. How often are security audits performed?
    3. Reviewing and purging unnecessary applications from the network
    4. Handling new employees entering the company
    5. Handling employees leaving the company
    6. Policies for disclosing sensitive information to persons outside the company
3. Access control systems
    1. Authentication methods
    2. Special access policies (e.g. password policies)
    3. Identifying which individuals have access to which systems and/or data
4. Risk assessment procedures
    1. Preventative measures and systems
        1. IDS, firewalls, proxy servers, data encryption, etc.
    2. VPN availability
    3. Business continuity planning (including testing)
    4. Physical security
    5. Electronic monitoring
    6. Policies for removing laptops and/or computer equipment from the premises

Section 2 should include any other questions that are specific for your particular organization. In other words, this section should be highly unique, to the extent that it would be impossible to provide a list of concepts here. Despite the list of concepts for Section 1 above, you should spend

quite a bit more time planning for Section 2.

NOTE: This deliverable is a list of questions only… **a "wish list**," if you will. Do not provide answers to the questions in this deliverable.

Reasonable expectation: around 2-3 pages