InfoSec exercise 4: identifying threats

In this exercise I will list only some of the more basic risks, vulnerabilities and countermeasures to keep the time needed to complete this task sensible. Exploring anything and everything would require weeks of time, better domain knowledge on the companies (systems) and much more people than just one student since the assignment is fairly unlimiting in possibilities and scope (rightly so, it has the possibility to make the assignment interesting).

Part A

- Owner: Company A
- Asset: Public website
- Threat agent: Hacktivist aiming to harass the company

Possible vulnerabilities and associated attack vectors

- Vulnerability: Badly coded form handling allowing SQL injection.
  - Attack vectors: Website's admin login form, comment form. Basically through any html form user has access to.
  - Countermeasures: Validate and/or sanitize every user input. Potential vulnerability here is that validation/sanitation is not correct or complete allowing unwanted data to pass through.

- Vulnerability: Insufficient resources to handle massive amounts of traffic
  - Attack vectors: Senging massive amounts of request (essentially DoSing) thus making the site impossible to be reached.
  - Countermeasures: Implementing load balancing technology with ability to drop denial of service requests. Potential vulnerabilities here are misconfiguration of the balancer or device breakdowns rendering the site impossible to be reached.

With a website there are a lot more possible vulnerabilities depending on technologies used and how they are configured. Ways to mitigate those vulnerabilities depends on the systems and resources available.

Possible threats

- Hacktivist adding propaganda to the website.
- Hacktivist removing or altering data (news, blogs etc) to create confusion within clients of the company.
- Hacktivist performing denial of service attacks to prevent users from reaching the site.

Part B

- Owner: Company B
- Asset: Customer credit card information
- Threat agent: Cyber criminal aiming for monetary profit

Possible vulnerabilities and associated attack vectors

- Vulnerability: basically the same SQL injection as in Part A comes to mind. No need to repeat it here fully though.

- Vulnerability: bad coding practices in externally accessible systems that use credit card information.
  - Attack vectors: Man-In-The-Middle attacks, Cross-Site Scripting techniques, or just guessing user IDs and getting the system to show someone else's data.
  - Countermeasures: System-specific but generally come down to knowing how to prevent these and search for these during development.

- Some general mitigation techniques would be to store credit card information in better protected internal server with no additional services running to reduce the attack surface. Even better would be if credit card information would not be needed at all, or at least that it would get deleted as early as possible.

Possible threats

- Cyber criminal sending fraudulent emails to possible customers of the company trying to phish for information.

- Cyber criminal extracting data from the credit card information database through a vulnerability.

Part C

- Owner: Company C
- Asset: CRM data
- Threat agent: Compromised insider responsible for customer relationships

Possible vulnerabilities and associated attack vectors

- Vulnerability: ability to extract customer data in bulk.
  - Attack vectors: Through normal system UI: (possibly unrestricted) export of customer data either in digital or analog (paper) form.
  - Countermeasures: Implement a firewall that tracks massive exports to external servers, not allowing bulk export from the system, tracking amounts of pages printed by each employee (and catching the anomalies there) and preventing use of external USB drives etc.

- Vulnerability: deleting or changing customer data.
  - Attack vectors: Through normal system UI: delete or modify customers orders and such data to make the company look bad (not delivering orders etc).
  - Countermeasures: Implement proper backup solutions, log user actions in the system, have ability to restore previous versions of data.

Possible threats

- Compromised insider extracting customer data to sell it or use it otherwise.
- Compromised insider deleting or changing customer data to cause harm (lost shipments, missing orders etc).