Welcome back!

In this exercise, you'll develop BCP and DR plans for *Geldcorp*. You'll work with a group of consultants, and each group will develop a plan for a different domain of the company.

In particular, you'll develop plans for one of the following realms:

* **Physical Environment**
* **Personnel**
* **Network**
* **Technology**
* **Security**

You should specify both a BCP and DR plan. The BCP plan will be for mild-to-moderate incidents, in which the business suffers damage but can maintain operations. The DR plan will be for situations where the business suffers a catastrophic incident that must be contained before operations can continue.

You'll summarize your plan in a Slide presentation. Your BCP and DR plans should cover the following:

* **Points and Modes of Failure**
  + Identify 2 points of failure or security weakness, and one major threat for each.
* **Projected Damages**: Explain how the business would be affected in the event each threat were realized.
* **Continuity/Recovery Plan**: For BCP, how the business could "patch" a mild/moderate incident to maintain operations during. For DR, explain how the business should prioritize its resources to recover from the reputational and operational damage of a catastrophic loss.

Use the information below to complete the slides. Read all of it, but only use the information relevant to your group's domain to create your plan.

Be sure to ask your instructors for help if you get stuck.

**Good luck!**

**About GeldCorp**

**Physical Environment**

* All office buildings have one main door and 2 secondary (back) doors.
* Each door has card access, but *GeldCorp* still experiences occasional tailgating.
* Servers at the data centers are in the main floor of each office, which is accessible from all wings of the building.

**Personnel**

* Aside from security culture training, none of the employees have any exposure to information security
* Technical employees and executives sometimes work remotely.
* Technical employees and executives are given Administrator accounts by default.
* Employee turnover is high.

**Network**

* *GeldCorp* has both wired and wireless networks.
* Visitors can connect to the guest network at the office. Employees often use this network.
* Employee workstations and laptops have VPN access to the corporate intranet.

**Technology**

* The company buys hardware and software and deploys them with default configurations.
* Some software applications are built internally by an in-house software development team.
* Each site on the corporate intranet requires employees to login, and sometimes different internal sites require a different login credentials.
* The company has experienced consistent virus and malware infections, due largely to phishing attacks.
* The company allows employees to connect their own devices to the office wireless networks.

**Security**

* *GeldCorp* has yet to implement your formal security policy recommendations. Currently, they have none.
* The company has experienced DDoS attacks in the past.
* No formal process exists for handling field issues or security incidents.