Thinking Like a General
A mission-oriented approach
Amazon Freezes Corporate Hiring in Its Retail Business
It is the latest tech company to pump the brakes on hiring amid growing economic concerns.

Google CEO Sundar Pichai hints at layoffs, says he ‘wakes up and worries’ about feds

Mark Zuckerberg says Meta will freeze hiring and cut costs

Walmart is also overstaffed. Microsoft lets hundreds of contractors go.
A wave of layoffs is sweeping through Netflix.
Meta is in a hiring freeze.
Google extended its hiring freeze.
CHANGING THREAT LANDSCAPE

- Supply Chain: 44%
- Digital Innovation: 41%
- Budget: 28%
- Talent Shortage: 25%
There isn't a company of any size that is immune from finding itself in the headlines.
The most common cyber breach fallacy is...
Fixing only the technical problem
There's no doubt that cyber events are becoming a business risk.
Where do you **start**?
Identify Internal & External Concerns to Revenue Streams
Enterprise Model

- Mission Objective
- Security Objective
- Business Unit
- Business Process

Mission Layer

Operational Layer

IT Model

- Node
- IT Services
- Software

Mission Risk Assessment Model
Identify Crown Jewels or Business Critical Systems
Mission Risk Assessment

MissionRisk = f(AssetRisk, MissionImpact)

- Hardware
- IT Services
- Applications
- Business Processes
- Operational Tasks
- Business Objectives
- Mission
There are over 186,000 known vulnerabilities in the Common Vulnerability and Exposure (CVE) Database.
There are 555 attack patterns documented in the Common Attack Patterns Enumerations and Classification (CAPEC) list.
Develop Defenses Using the DIMFUI Taxonomy
Focus on the effects of the attacks

**Degradation:** An attacker causes a reduction in the performance of an IT resource of the system. Examples of degradation are reduced network bandwidth, a slower computer, or the lower quality of some information.

**Interruption:** An attacker causes an information asset of the system to become unusable, unavailable. Interruption can be thought of as complete degradation.

**Modification:** An attacker causes a change in the data, protocol, software, or hardware of an IT resource.

**Fabrication:** An attacker inserts false information or components into a system. Examples are counterfeit hardware or software that can perform unexpected activities.

**Unauthorized Use:** An attacker uses system resources for illegitimate purposes.

**Interception:** An attacker gains unauthorized access to information or assets. An example is an attacker finding credit card in the memory of a computer.
Where can you find me?

Dr. Bill Souza | LinkedIn

Dr. Bill Souza | @DrBillSouza

The Doctor’s Advice @ Apple Podcast

The Doctor’s Advice @ Youtube Channel