INFM612 - FINAL PROJECT PRESENTATION

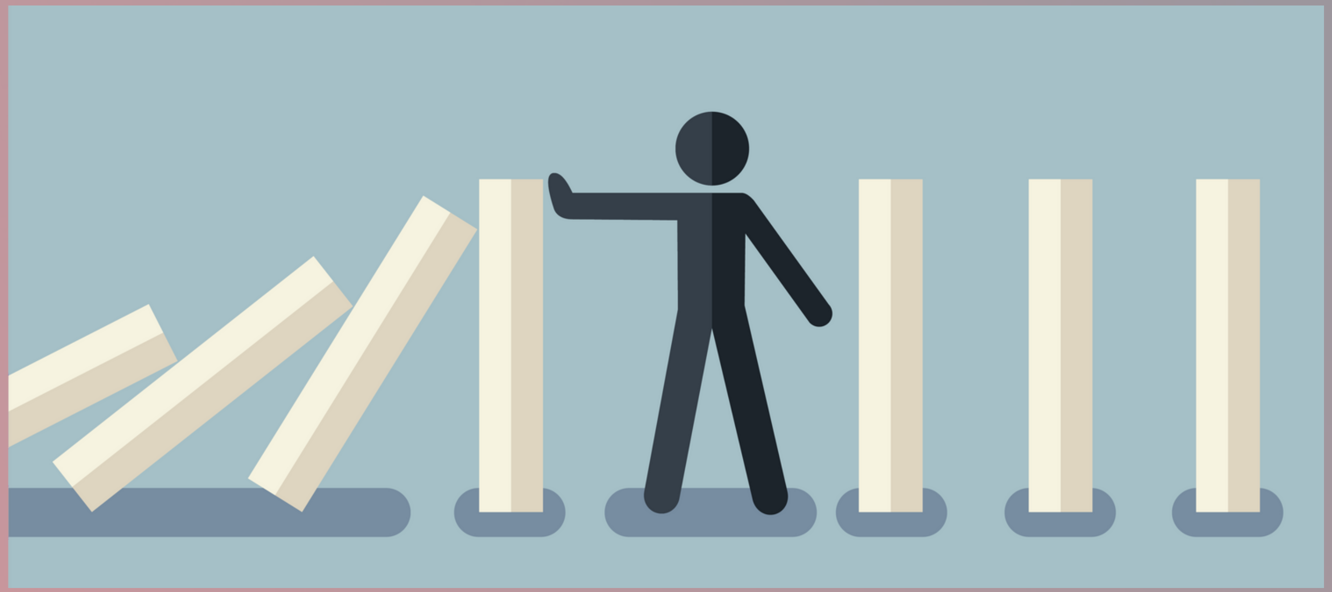
BUSINESS CONTINUITY MANAGEMENT IN THE AGE OF DISRUPTIONS

-STRATEGIES FOR PLANNING AND RESPONSE-

DATE OF COMPLETION: May 14, 2023

TEAM 05
PRANAV TEJASVI ADIRAJU
ASMITA SAMANTA
DHIRAJ LAHOTI
SHARVIL SHASTRI
RITIKA NAMILIKONDA

Business Continuity Plan



- A set of procedures and strategies designed to help a business or organization prepare for and respond to unexpected events that could disrupt normal operations.

- Essential for any organization because it helps ensure that critical business functions can continue during and after unexpected events, such as natural disasters, cyberattacks, pandemics, or other crises

- Ensures that organization can continue to provide products and services to their customers, even in the midst of a crisis

Importance of BCP

1. Ensures Business Resilience
2. Minimizes Financial Losses
3. Protects Organization's Reputation
4. Enhances Compliance
5. Minimizes Downtime
6. Protects our Data

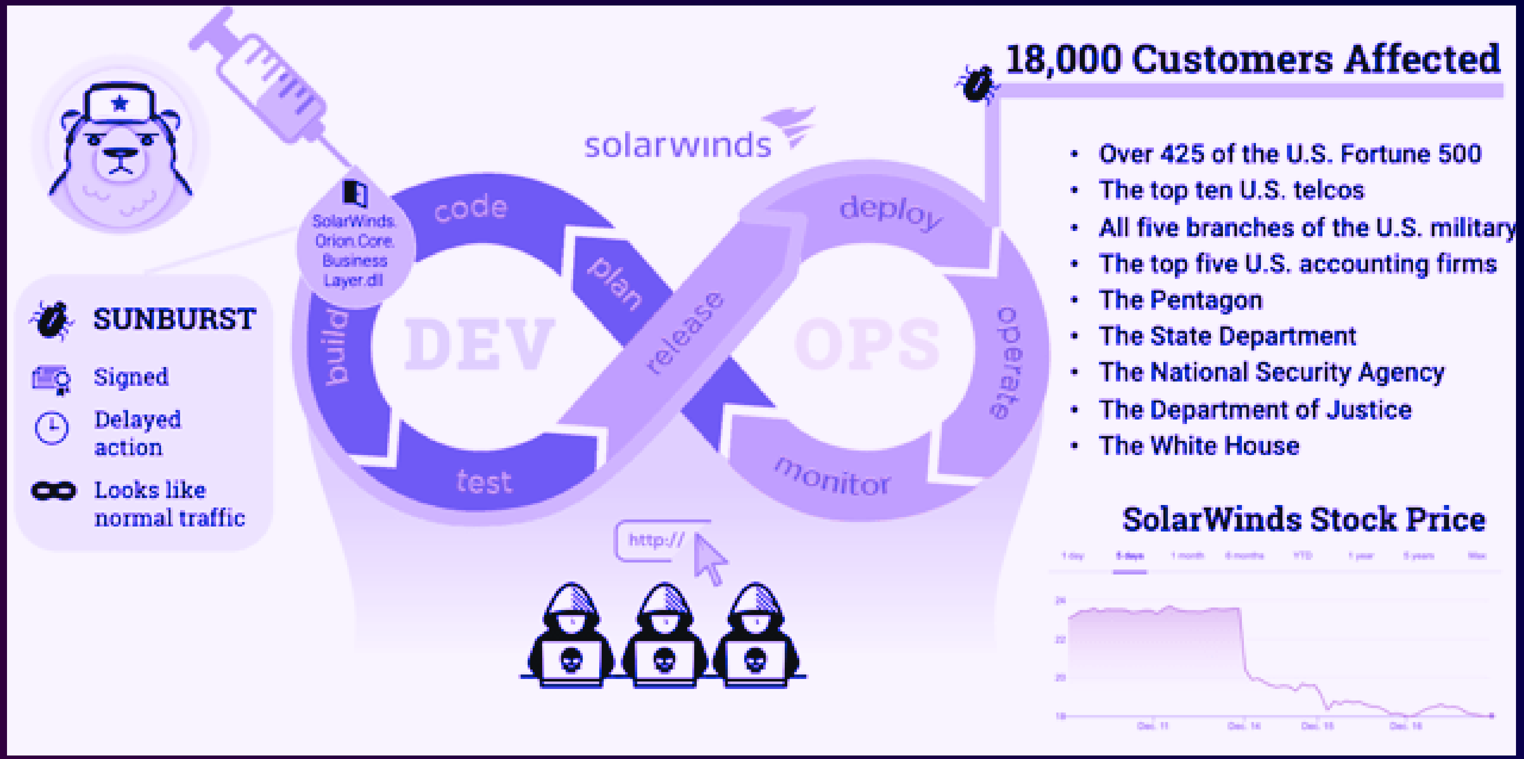
BCP IN CYBERSECURITY

- Cyber incidents can disrupt business operations.
- BCP ensures continuity, mitigation, and recovery.
- Maintains essential functions during incidents.
- Minimizes the impact of cyber threats.
- Restores normal operations swiftly.
- Crucial for business resilience in cybersecurity.

BENEFITS OF BCP IN CYBERSECURITY

1. Minimize downtime
2. Protects sensitive data
3. Reduces financial losses
4. Ensures compliance
5. Enhances resilience

Solarwinds Supply Chain Attack(2020)



- Over 425 of the U.S. Fortune 500
- The top ten U.S. telcos
- All five branches of the U.S. military
- The top five U.S. accounting firms
- The Pentagon
- The State Department
- The National Security Agency
- The Department of Justice
- The White House

- Hackers injected malware into SolarWinds' software updates
- Malware remained stealthy and avoided detection
- Targeted several high-profile organizations
- The attack exfiltrated sensitive data
- The attack initiated the nationwide adoption of better cybersecurity practices

Solarwinds Supply Chain Attack(2020)

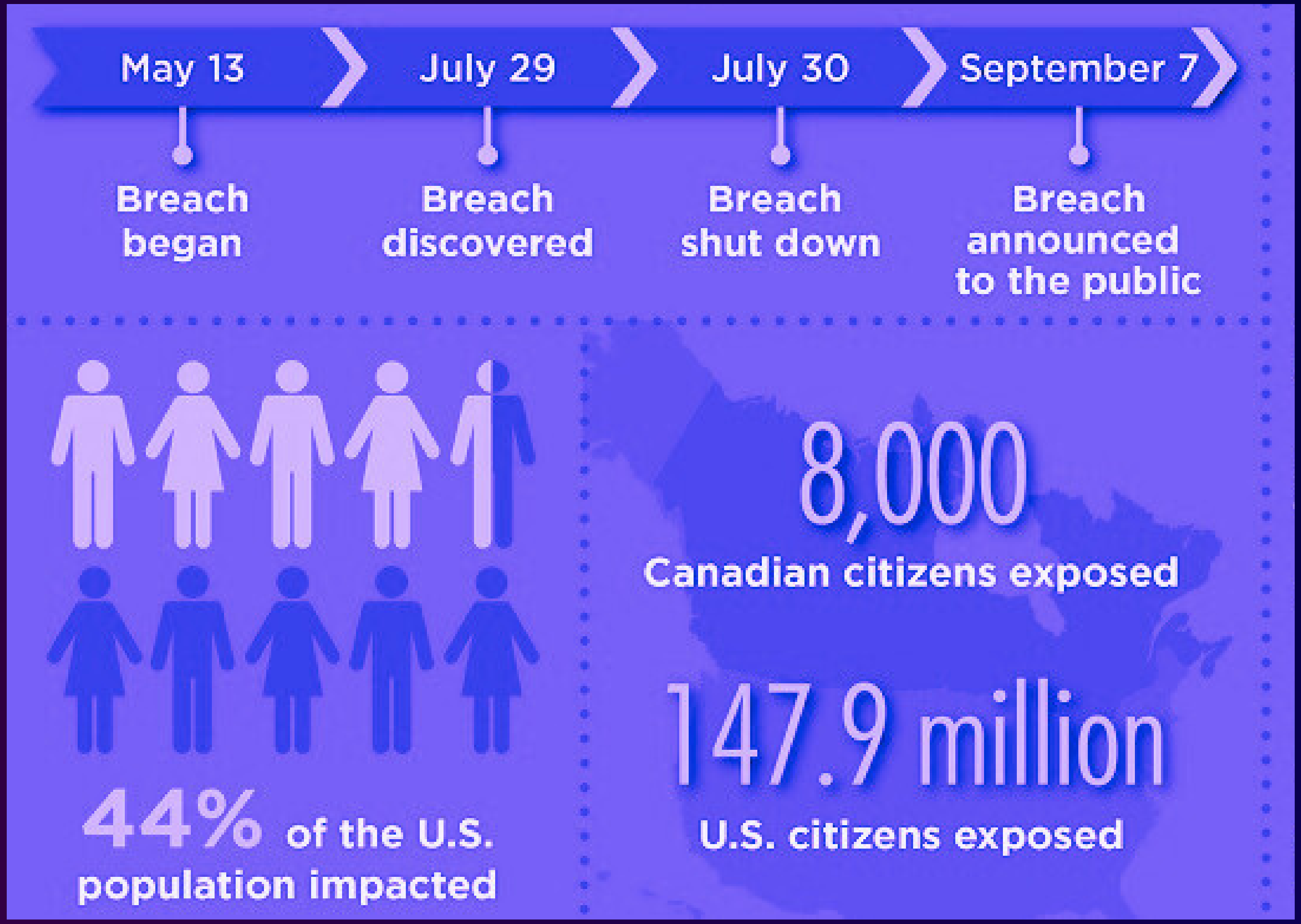
Lessons Learnt

- Cyber attacks can exploit supply chain vulnerabilities
- Advanced persistent threats can go undetected
- Importance of transparency and collaboration
- The critical role of incident response planning

Changes in BCP

- Ensure supply chain security
- Implement a zero-trust architecture
- Strengthen threat detection and response capabilities
- Foster a culture of cybersecurity awareness
- Collaborate and share information

Equifax Data Breach (2017)



- Hackers exploited a vulnerability in Equifax's web application software
- The attack exfiltrated sensitive data for weeks
- The company was slow in responding to the breach
- Lawsuits were filed against Equifax along
- Equifax invested in better cybersecurity practices

Equifax Data Breach (2017)

Lessons Learnt

- The importance of vulnerability management
- The risk of insider threats
- The need for a robust incident response plan
- The importance of regular cybersecurity training

Changes in BCP

- Regular risk assessments
- Robust cybersecurity policies and procedures
- Incident response plan
- Backup and recovery plan
- Vendor and third-party risk management
- Cybersecurity insurance
- Stronger oversight and accountability

Creating an Ideal BCP: Initial Steps

- **RISK ASSESSMENT:** IDENTIFY POTENTIAL CYBER THREATS AND VULNERABILITIES TO PRIORITIZE PROTECTION.
- **DEFINE ROLES AND RESPONSIBILITIES:** CLEAR DEFINITION OF DUTIES FOR INDIVIDUALS AND TEAMS INVOLVED IN BCP.
- **INCIDENT RESPONSE PLANS:** OUTLINE STEPS TO TAKE IN THE EVENT OF A CYBER INCIDENT FOR EFFECTIVE CONTAINMENT AND MITIGATION.

Creating an Ideal BCP: Continuous Actions

- **REGULAR BACKUP OF CRITICAL DATA:** ENSURE INTEGRITY AND ACCESSIBILITY OF BACKUPS.
- **IMPLEMENT ACCESS CONTROLS:** PROTECT SENSITIVE DATA AND CRITICAL SYSTEMS WITH EFFECTIVE MEASURES.
- **EMPLOYEE TRAINING:** REGULAR TRAINING ON CYBERSECURITY BEST PRACTICES AND BCP ROLES.
- **TEST AND UPDATE THE BCP:** REGULAR TESTING AND UPDATES TO KEEP THE BCP EFFECTIVE AND UP-TO-DATE.

AI in Cybersecurity Incident Response & Vulnerability Management

- **Automating Incident Response with AI**
  - Machine learning algorithms can detect and respond to cyber threats in real-time.
  - IBM's Watson for Cyber Security and Darktrace's Enterprise Immune System are prime examples.
- **AI in Vulnerability Management**
  - AI can identify, prioritize vulnerabilities and recommend remediation strategies.
  - Qualys Vulnerability Management automates network scanning, prioritization, and patch recommendation.

AI in Disaster Recovery Planning & Fraud Detection

- **Automating Disaster Recovery with AI**
  - AI enables automatic data backup, recovery, and replication.
  - Commvault's Disaster Recovery solution exemplifies AI's role in disaster recovery.

- **AI in Fraud Detection**
  - AI analyzes large data sets to identify fraudulent activity patterns.
  - Visa uses AI to analyze transactions in real-time, blocking potential fraud.

Metrics to implement an ideal BCP w.r.t cybersecurity

- Recovery Time Objective (RTO)
- Recovery Point Objective (RPO)
- Mean Time to Detect (MTTD)
- Mean Time to Respond (MTTR)
- Testing Frequency
- Employee Awareness
- Incident Response Plan Effectiveness

How to promote awareness about BCP?

- Training and Education
- Communication
- Involvement

- Drills and Exercises
- Awareness Campaigns
- Senior Management Support