IVK Debate-
Pro Non-disclosure of Systems Outage

PMBA - MIS 5402 - Managing Technology & Systems - Spring 2017

Eisha Moore

Opening Arguments

- Non-consensus on the cause of systems outage
- Potential damage from mislabeling the event
- Aftermath of event open to broad interpretation
- No environment is free from systems outages or security breaches
- Disclosure is required only if customer data is suspected to be compromised
- Over-action versus under-action

DDOS Attacks are Common

- IVK implemented DDOS mitigation
- Referenced list of source IPs and protocols for redirecting traffic during the attack/event
- Established contacts with ISP, IDS, firewall, systems, and network and development teams.

Database Systems Failure

- Security breach or Software issue?
- Renamed database files are not ideal but fairly routine
- Activity logs verification
- No automated process operates at 100% without errors

Recommendations to the Leadership Team
The 'Do Nothing' Strategy'

- Production systems shut down for "preventive" maintenance for 3-4 days
    I. PR framing includes systems upgrade, commitment to security, and service upgrade
    II. Rebuild critical production systems from development files
- Contact customers who's records have been accessed within a certain time frame
    I. Careful customer contact strategy that includes narrative regarding commitment to customer security

Business Continuity Response to Systems Outage

- Fast track security projects-scope and costs
- Update Systems Recovery Procedures
- Create/Update Data Recovery Procedures
- Scheduling Cloning
- Build parallel mirror site from dev files
- Document IVK IT infrastructure details, including business owners, IP addresses and circuit IDs; prepare a network topology diagram and asset inventory.