Xbox: Information Risk Management

An Analysis of Previous Incidents and Potential Risks

Growth Causes Complications

In recent years the games industry has grown significantly, with an increased presence of online platforms.

The requirement of 24 hour availability of online services has made way for numerous complications.

Key Incident: 2011 PSN Hack

- 77 Million users personal data compromised.
- Service unavailable for nearly an entire month.
- One of the largest breaches at its time.
- Caused upheaval among policies in regards to Cyber Information Risk.

PSN Hack: Lessons to be Learned.

- Despite the damage, Sony recovered.
- Such a recovery was possible due to openness and a “Welcome back Campaign”.

Incidents: Lizard Squad DDOS

- Throughout 2014 a sophisticated hacker group performed numerous high profile planned DDOS attacks.

- Such attacks compromised numerious platforms availability.

Incident: Insider Leaks

- During the development of the Playstation 5, Sony suffered numerous leaks.

- All of the leaks happened during internal events involving 3rd parties.

Methodology

- A combination of FAIR and ISO.
- FAIR is good for identifying threats, risks, and all of their elements.

- ISO is good for deciding and justifying controls.

- Using them in conjunction creates a singular strong methodology.

Assets and Personnel

- Data Centres
  - Microsoft Azure
  - Operating Personnel
- Public Facing Workers

Threat Actors and Communities

Cyber Criminals

- External
- Extremely Diverse in skill level

- Lizard Squad is our previously noted example.
  - Ideological?
  - Erratic?

Employees

- Numerous different actors.
- Two motivations
  - Revenge
    - Desiring to cause damage to infrastructure
  - Financial
    - Stealing data in order to sell it.
- Leakers can occur in any of these.

Measuring Risk
A Few Examples

Distributed Denial of Service Attack

- Threat Event Frequency: Moderate.
- Threat Capability: Very High.
- Controls: Response Strategy, Geographic Distribution.
- Control Strength: Very High (90%).
- Vulnerability: Moderate Vulnerability (65%).
- Loss Event Frequency: Moderate (50%).
- Probable Loss Magnitude: Significant (100,000+).

Critical Network Breach

- Threat Event Frequency: Very Low: One every ten years.
- Threat Capability: Very High.
- Controls:
  - Response Strategy.
  - Event Logging.
  - Admin and Operator Logs.
  - Controls Against Malware.
  - Restrictions on Software Installation.
  - Network Controls / Security / Segregation.
- Control Strength: High.
- Vulnerability: High.
- Loss Event Frequency: Very Low.
- Probably Loss Magnitude: Severe.

Questions?