Minimizing Business Disruption After a Cyberattack

Cyber Security Challenges, Threats and Strategies Symposium
University of Bahrain
21st September 2016

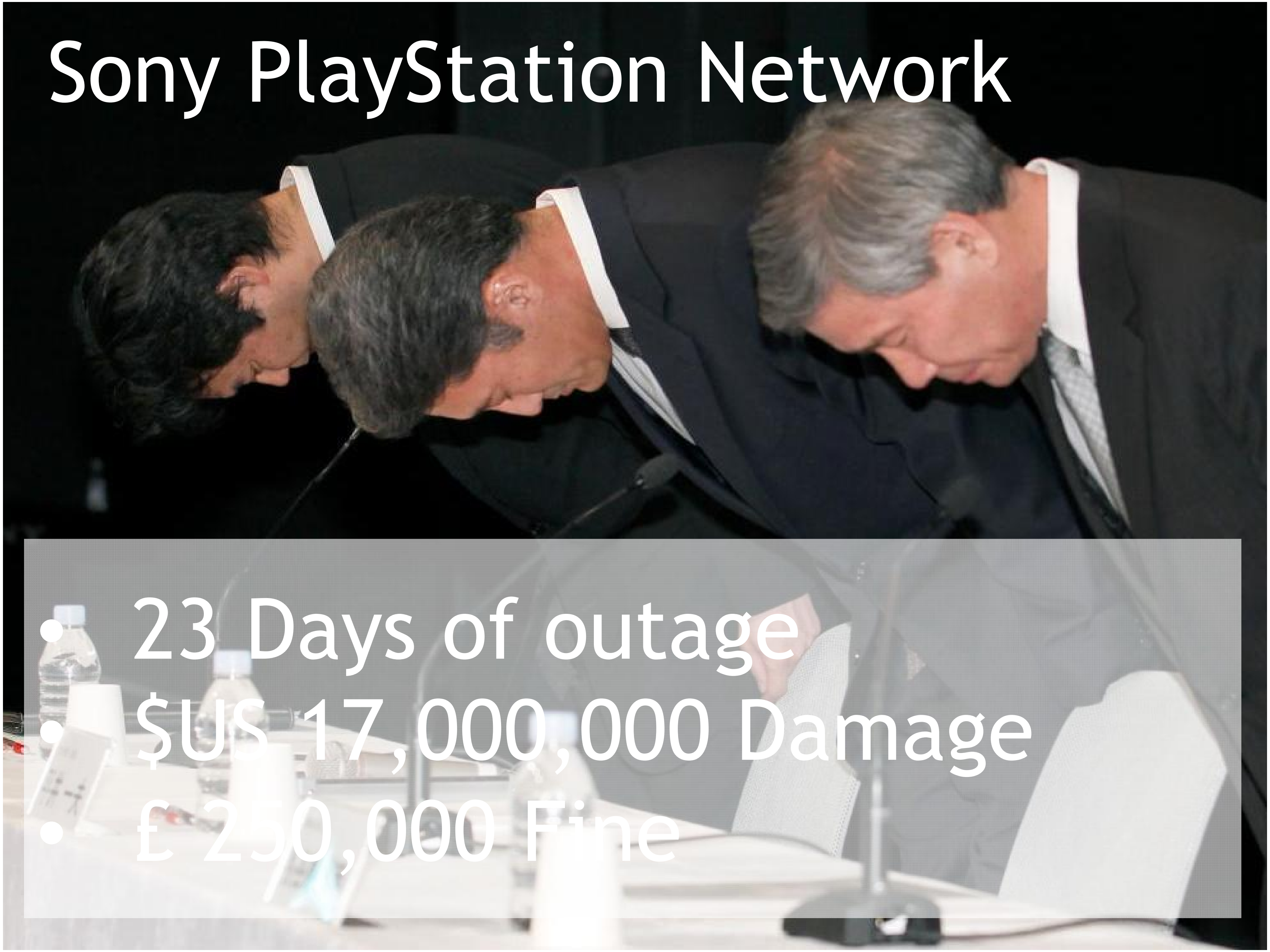
By: Ahmed Albalooshi, CISA, CISM, CGEIT.
First Vice President – IT
Al Baraka Banking Group
aalbalooshi@albaraka.com

Agenda

- *Why prepare for Cyberattacks?*
- *How to prepare for Cyberattacks?*

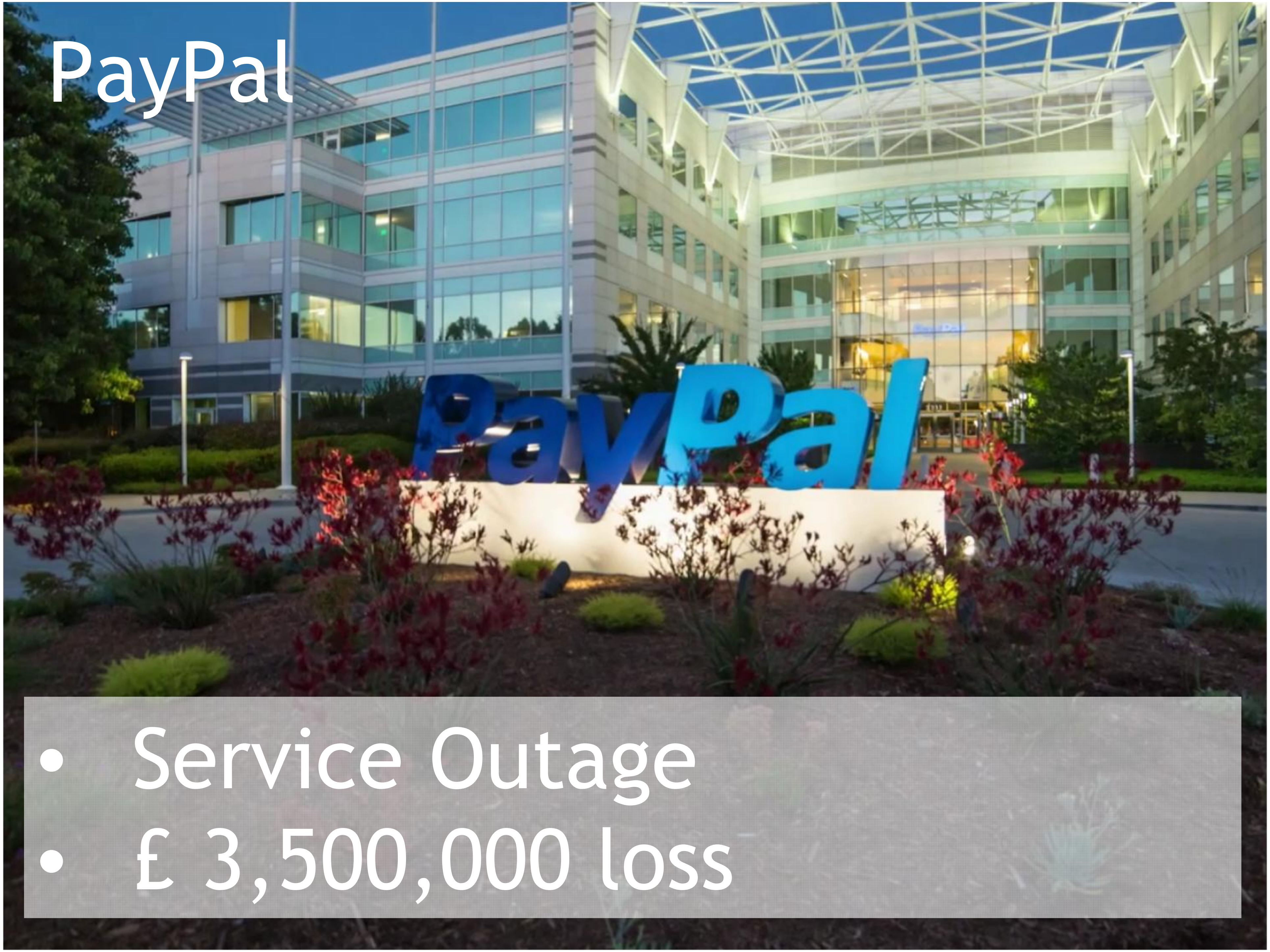
Why prepare for Cyberattacks?

Sony PlayStation Network



- 23 Days of outage
- $US 17,000,000 Damage
- £ 250,000 Fine

PayPal



- Service Outage
- £ 3,500,000 loss

Bangladesh Central Bank

- US$ 81,000,000 heist

London Stock Exchange welcomes
Tuesday 21 October 2014 08:03
World Indices
HM Government
UK Government offshore RMB bond issuance
RISERS
The launch of the UK Government's RMB bond
Focus on Sweden and the Baltic
BRITVIC 618.00 0 (0.0%)
G4S 248.90 -1.00 (-0.4%)
AZIMUT 17.27 -0.17 (-1.0%)
INTL CONSOL AIR 359.50

London Stock Exchange

- 2 hours downtime

“Prepare for Cyberattacks”

Central Bank of Ireland

“By 2020, 30% of effected firms will spend 2 months cleansing data & Systems”

Gartner

“205 days: the average time for firm to detect that they were infiltrated”

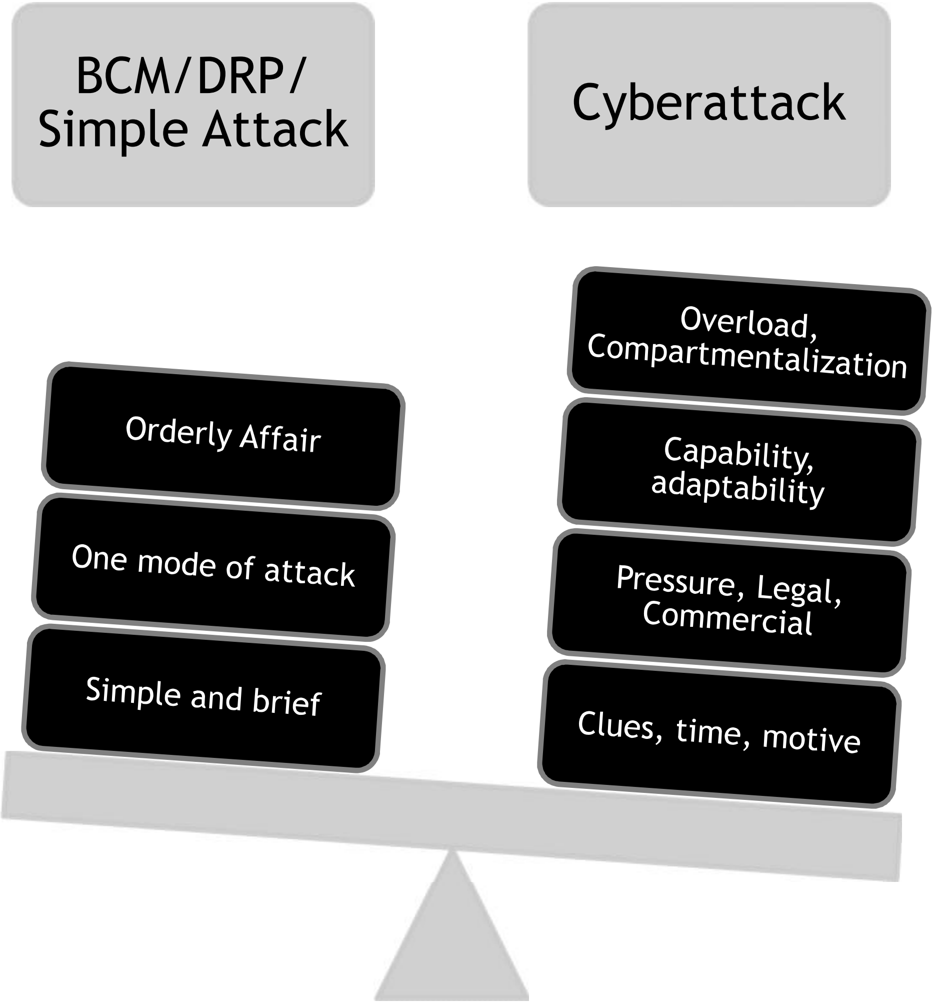
FireEye

How to prepare for Cyberattacks?

Understanding the Nature of Cyberattacks

Gartner: "A Cyberattack is a Street fight"

Understanding the Nature of Cyberattacks



BCM/DRP/ Simple Attack

Cyberattack

Orderly Affair

One mode of attack

Simple and brief

Overload, Compartmentalization

Capability, adaptability

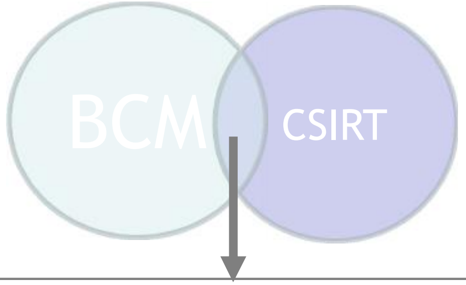
Pressure, Legal, Commercial

Clues, time, motive

Uncertainties:

- The extent of infiltration is yet unknown
- Stay live for investigation and Forensic
- Avoid shutdown that will alert cyberattacker
- Backup and DR might be also infected

Preparing for Cyberattacks



Integrating established BCM with existing CSIRT

Planning

- Joint Workgroup between BCM & CSIRT
- Develop one Crisis Management Team
- Expand CSIRT to include BCM Team
- Add cyberattack as a scenario in BIA
- Align to standard and best practices
- Develop work-around procedures for offline
- Exercise plans jointly (BCM & CSIRT)
- Develop Data protection strategy
  (malware scanning, consistency testing, data integrity checking)
- Leverage BCM Tools for CSIRT
- Establish communication plan & services
- Plan for corrupt/lost data

Response & Recovery

- CSIRT should advise the Crisis Team
- Monitor the timeline of response Vs. RTO
- Assess the integrity of applications and backup
- Perform mop-up operations and feedback

Response and Recovery Standard/Best Practice

- ISO 22320:2011 Societal Security — Emergency management — Requirements for Incident Response
- ISO 22301:2012 Societal Security — Business Continuity Management Systems — Requirements
- ISO 22313:2012 Societal Security — Business Continuity Management Systems — Guidance
- ISO/IEC 27031:2011 Information Technology — Security Techniques — Guidelines for Information and Communication Technology Readiness for Business Continuity
- ISO/IEC 27032:2012 — Information Technology — Security Techniques — Guidelines for
- Cybersecurity
- ISO/IEC 27001 — Information Security Management
- ISO/IEC 27035:2011 — Information Technology — Security Techniques — Information Security
- Incident Management
- BS 11200 Crisis Management — Guidance and Good Practice
- U.S. Department of Homeland Security National Incident Management System (NIMS)/Incident Command System (ICS)
- NIST SP 800-61 Rev. 2, Cybersecurity Incident Handling Guide (August 2012)
- Expectations for Computer Security Incident Response

In Summary

- *A successful cyberattack can shutdown your business operations for a long time causing information leak, financial loss, reputational damage, etc.*
- *Backup systems, applications, data and disaster recovery might also be infected derailing you from BCM, RTO and RPO.*
- *Integrating BCM and CSIRT planning, response and recovery are the best approach to minimize disruption of a cyberattack.*

REUTERS