Cyber Security and BCM
No one is immune!

Business Continuity Awareness Week 2013
Sydney
Our discussion today

What is Cyber Security?

What happens if you're not prepared…

Cyber Security happens locally and internationally

As BCM Professionals, what do we need to consider

What happens if you are prepared…

Building Resiliency and Better Outcomes
What is Cyber Security?

- In general, cyber security incidents include but are not limited to:
  - attempts to gain unauthorised access to a computer system or its data
  - unwanted disruption or denial of service
  - unauthorised use of a system for processing or storing data
  - changes to system hardware, firmware or software without the knowledge or consent of the system owner

Cyber Security incidents can be:
- Personal gain
- Sovereign gain
- Malicious gain
What happens when you’re not prepared……

Cyber Security Impacts

• Cyber Security events may not always occur immediately
  – Tracers and malware can be in place for months/years before the event occurs

• Attacks can originate locally or internationally

• Cyber security can impact organisations:
  – Brand and reputation
  – Market price / market share
  – Financially
  – Customers / Clients / Third Party Suppliers

According to the latest BCI research -

65% of firms are ‘Concerned’ or ‘Extremely Concerned’ about a cyber attack
It happens locally and internationally

1 in 5 companies in general suffered a breach - 2012 National Cyber Crime and Security Survey
Use Case

Distribute IT

- The cyber-attack that crippled Melbourne-based web hosting provider Distribute.IT has left thousands of customers furious, with the data of almost 5,000 websites now deemed completely unrecoverable
- Hackers permanently obliterated files and websites during a devastating half hour of infiltration (Saturday night on June 11, 2012)
- This event resulted in the company going-out-of-business, due to impact on customer and reputation damage and being acquainted by Netregistry Group

Lesson Learnt:

- Consider the risks of the cloud – understand your hosting provider BC / IT DR capabilities and understand the risks of having a hosted solution in the cloud
- Get your security on track – understand your IT infrastructure and the security vulnerabilities
- Keep up to date - Keeping up to date with the latest news in Trojan bugs and Exchange servers risks
## Cyber Security Maturity Model

How effectively does your organisation prepare for, become aware of, and respond to cyber threats?

### Cyber Security Maturity Levels

<table>
<thead>
<tr>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT BC &amp; DR Exercises</td>
<td>IT Cyber Attack Simulations</td>
<td>Business-Wide Cyber Attack Exercises</td>
<td>Sector-Wide &amp; Supply Chain Cyber Attack Exercises</td>
<td>Cyber Attack Preparation</td>
</tr>
</tbody>
</table>

### Proactive Threat Management

- Blissful Ignorance
- Transformation
- Operational Excellence

### Blissful Ignorance

- Media & SMEs
- Consumer Business & Life Sciences
- Retail Banks & Energy Providers
- Investment Banks
- Military & Defence

### Transformation

- Acceptable Usage Policy
- General Information Security Training & Awareness
- Targeted Intelligence-Based Cyber Security Awareness
- Business Partner Cyber Security Awareness

### Operational Excellence

- Government / Sector Threat Intelligence Collaboration
- Real-time Business Risk Analytics & Decision Support
- Business Partner Cyber Security Awareness
- Cyber Attack Preparation

### Cyber Security Maturity Model Details

- **Basic Network Protection**
  - Ad Hoc Infrastructure & Application Protection
  - Enterprise-Wide Infrastructure & Application Protection
  - Identity-Aware Information Protection
  - Adaptive & Automated Security Control Updates
  - Asset Protection
  - Security Event Monitoring
  - Internal Threat Intelligence

- **IT Service Desk & Whistleblowing**
  - Security Log Collection & Ad Hoc Reporting
  - 24x7 Technology Centric Security Event Reporting
  - External & Internal Threat Intelligence Correlation
  - Cross-Channel Malicious Activity Detection

- **Traditional Signature-Based Security Controls**
  - Periodic IT Asset Vulnerability Assessments
  - Automated IT Asset Vulnerability Monitoring
  - Targeted Cross-Platform User Activity Monitoring
  - Tailored & Integrated Business Process Monitoring

- **IT BC & DR**
  - Acceptable Usage Policy
  - General Information Security Training & Awareness
  - Targeted Intelligence-Based Cyber Security Awareness
  - Business Partner Cyber Security Awareness

- **Ad Hoc System / Malware Forensics**
  - Ad-hoc Threat Intelligence Sharing with Peers
  - Government / Sector Threat Intelligence Collaboration
  - Global Cross-Sector Threat Intelligence Sharing

- **Enterprise-Wide Infrastructure & Application Protection**
  - Network & System Centric Activity Profiling
  - Workforce / Customer Behaviour Profiling
  - Real-time Business Risk Analytics & Decision Support
  - Business Partner Cyber Security Awareness

- **Government / Sector Threat Intelligence**
  - Commercial & Open Source Threat Intelligence Feeds
  - Criminal / Hacker Surveillance
  - Baiting & Counter-Threat Intelligence
  - Global Cross-Sector Threat Intelligence Sharing

- **Technology & Business Intelligence**
  - Global Cross-Sector Threat Intelligence Sharing
  - Real-time Business Risk Analytics & Decision Support
  - Business Partner Cyber Security Awareness

- **Adaptive & Automated Security Control Updates**
  - Targeted Cross-Platform User Activity Monitoring
  - Tailored & Integrated Business Process Monitoring

- **E-Discovery & Forensics**
  - Automated Malware Forensics & Manual Electronic Discovery
  - Automated Electronic Discovery & Forensics
  - Real-time Business Risk Analytics & Decision Support
  - Business Partner Cyber Security Awareness

- **Intelligence Collaboration**
  - Government / Sector Threat Intelligence Collaboration
  - Global Cross-Sector Threat Intelligence Sharing
  - Real-time Business Risk Analytics & Decision Support
  - Business Partner Cyber Security Awareness

- **E-Discovery & Forensics**
  - Automated Malware Forensics & Manual Electronic Discovery
  - Automated Electronic Discovery & Forensics
  - Real-time Business Risk Analytics & Decision Support
  - Business Partner Cyber Security Awareness

- **Real-time Business Risk Analytics & Decision Support**
  - Real-time Business Risk Analytics & Decision Support
  - Business Partner Cyber Security Awareness
  - Cyber Attack Preparation

- **Business Partner Cyber Security Awareness**
  - Targeted Intelligence-Based Cyber Security Awareness
  - Business Partner Cyber Security Awareness
  - Cyber Attack Preparation

- **Behavioral Analytics**
  - Criminal / Hacker Surveillance
  - External Threat Intelligence
  - Internal Threat Intelligence
  - Cyber Attack Preparation

- **Training & Awareness**
  - Ad-hoc Threat Intelligence Sharing with Peers
  - Secure Online Monitoring
  - Online Brand & Social Media Policing
  - Cyber Attack Preparation

- **Situational Awareness of Cyber Threats**
  - Secure Online Monitoring
  - Online Brand & Social Media Policing
  - Cyber Attack Preparation

- **Cyber Security Maturity Levels**
  - Level 1: IT BC & DR Exercises
  - Level 2: IT Cyber Attack Simulations
  - Level 3: Business-Wide Cyber Attack Exercises
  - Level 4: Sector-Wide & Supply Chain Cyber Attack Exercises
  - Level 5: Cyber Attack Preparation

### Key Cyber Security Practices

- **IT BC & DR Exercises**
- **IT Cyber Attack Simulations**
- **Business-Wide Cyber Attack Exercises**
- **Sector-Wide & Supply Chain Cyber Attack Exercises**
- **Cyber Attack Preparation**

### Cyber Security Maturity Levels

- **Level 1**
  - Basic Network Protection
  - Ad Hoc Infrastructure & Application Protection
  - Enterprise-Wide Infrastructure & Application Protection
  - Identity-Aware Information Protection
  - Adaptive & Automated Security Control Updates
- **Level 2**
  - Asset Protection
  - Security Event Monitoring
  - Internal Threat Intelligence

### Cyber Security and BCM

© 2013 Deloitte Touche Tohmatsu
As BCM Professionals, what do we need to consider

The leading threat of concern in 2013 is unplanned IT and telecommunication outages, with 70% of organisations surveyed stating they were extremely concerned or concerned about this threat. Second to a data breach at 66%

Horizon Scan 2013 Survey Report
No such thing as hacker-proof…… building capability matters

- Based on current cyber threats, a range of scenarios can be used to test specific plans, rehearse interactions between teams or functions and challenge assumptions.
- Examples of potential scenarios, included for illustrative purposes only:

  - **DDoS attack**
    - Tests the technical team and organizations response to an attack on its own systems at a peak time
    - ‘Bottom up’ notification from technical team

  - **Public hoax**
    - Tests the technical teams ability to expedite resolution by testing key verification channels
    - ‘Bottom up’ notification from customer care

  - **Financial data leak**
    - Tests the crisis management of a ‘top down’ incident where notification is received via an infrequent route
    - Focus on regulatory, legal and reputational issues

  - **Attack on an outsourced provider**
    - Tests the team’s response to an incident where a level of control is lost due to the attack being targeted on the supplier

  - **Malware discovery**
    - Tests the technical team’s forensic capabilities and the business’s strategy on disclosure and resource impacts

  - **Insider attack on infrastructure**
    - Tests the technical response and business stance on information management
What happens when you are prepared.....


http://www.youtube.com/watch?v=l_XOrcBxy-E
Group Discussion

• Is cyber security being considered within your organisation?

• Have you been involved in a cyber security response?
  – What have been your experiences?

• What activities / steps are you currently taking in this space with your BCM program?
  – Cyber Security Crisis Management Exercise?
  – Increasing awareness about cyber security disruption events?
Where to go next?

- **CERT Australia**  
  *Australia’s National Computer Emergency Response Team*  

- **Cybersmart Website**  

- **Industry information**  
  - The BCI - [http://www.thebci.org/](http://www.thebci.org/)  
    there are a lot of sources available……
General information only

This presentation contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively the “Deloitte Network”) is, by means of this presentation, rendering professional advice or services.

Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this presentation.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/au/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte’s approximately 195,000 professionals are committed to becoming the standard of excellence.

About Deloitte Australia

In Australia, the member firm is the Australian partnership of Deloitte Touche Tohmatsu. As one of Australia’s leading professional services firms. Deloitte Touche Tohmatsu and its affiliates provide audit, tax, consulting, and financial advisory services through approximately 6,000 people across the country. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. For more information, please visit our web site at www.deloitte.com.au.

Liability limited by a scheme approved under Professional Standards Legislation.

Member of Deloitte Touche Tohmatsu Limited
© 2013 Deloitte Touche Tohmatsu