Not if, but When: **Proactive Cyber Claims Preparation**

Thursday 1 October 2020 10:00am AEST









Welcome

Jennifer Richards Managing Director - Specialties Australia



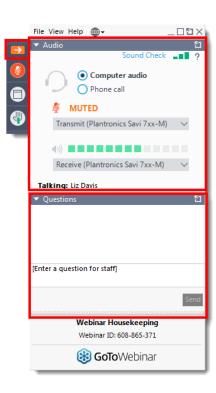






Housekeeping

- Today's session is being recorded
- You have joined in "listen-only" mode
- Please feel free to ask questions throughout the presentation utilising the 'Questions' window on your control panel
- We will endeavour to answer these as we progress through the session









Today's presenters



CHRIS MCLAUGHLIN Director, Cyber Solutions Group Aon



MICHAEL PARRANT Cyber Insurance Practice Leader Aon



JOHN MORAN Partner Clyde & Co



MOLLY DAY ANZ Cyber Threat Intelligence Lead Accenture



MARK SAYER APAC Cyber Defence Lead Accenture









Pitfalls in cyber claims

Chris McLaughlin

Aon Cyber Solutions







Pitfalls when managing your cyber claim

Learnings from recent claims

Betterment

Be mindful of waiting periods, periods of cover, betterment vs restitution

Adjustment

Openness and transparency from the adjusters to allow constructive dialogue

Incident Response

Aligning insurer, adjuster, indecent response, triage and rehearsal as part of **BAU** planning

Claims Prep Expenses

Clarity from all parties on claims prep limit and experience needed

Policy Wording

Understanding the policy features that you need to have awareness of









Claims protocols

Michael Parrant

Aon Cyber Solutions







Claims protocols

What does a claims protocol consist of?

Insurance Claims

Negotiate on behalf of the client to protect organizations from financial impact of a cyber incident

Business Interruption Claims Preparation

Address the business interruption coverage not typically offered by cyber insurance policies by adding industry leading terms

eDiscovery

Analyze evidence to target, analyze, understand, and present the key issues in a reasonable, efficient, and defensible manner



Incident Response

Respond to the incident, create an investigation strategy, contain the incident while preserving evidence, and communication confidently with stakeholders

Digital Forensics

Find, preserve, and analyze relevant data to provide definitive, fact-based conclusions for our clients. their counsel, opposing counsel, and the courts









Incident response and the claims process

John Moran

Clyde & Co







The incident response and claims process

Key stages

Incident response



Report incident to broker / breach coach / insurer



Triage incident and provide mitigation advice to contain, investigate and respond to incident



Manage and coordinate internal and external stakeholders including third party vendors



Breach coach to provide ongoing reporting and assistance

IT security / forensic review

Claims, defence and regulatory investigations



Respond to regulatory investigations



Defend third party claims



Pursue recovery actions

Cyber incident

< 1-3 months

3+ months

> 6 years









Lessons from incident response

Molly Day & Mark Sayer

Accenture







Cyber resiliency is about minimising the impact from cyber attacks

Key learnings from Accenture's global Cyber Investigations and Forensic Response team

Planning and Simulation

Train like you fight, fight like you train. **Build incident** response memory muscle

Incident Response

What happens during a typical incident response

Threat Intelligence

How threat intelligence can help you make better decisions

Containment & **Eradication**

Planning to eject the threat, impacts on operations and personnel

Recovery & **Transformation**

Policy features that you need to have awareness of









Claims process best practices







Key takeaways



Implement a claims protocol

Ensure that you have a claims protocol worked out and everyone knows the part they play



Think about your claim early

Start planning for a claim from the inception of the policy, understand how the policy will react to claims



Integrate cyber insurance into incident response

Include insurance into your incident response plans. Know the who, what, when and why of your partners



Rehearse the use of cyber insurance

Include the cyber insurance lifecycle into your incident response plan testing including testing of the claims process









Thank you for your attendance







The information contained herein and the statements expressed are of a general nature and may not apply to particular factual or legal circumstances. The materials do not constitute legal advice or opinions and should not be relied upon as such. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Copyright Notice

Copyright © 2020 Aon Corporation. All rights reserved. No part of this document may be reproduced in any form, including video recording, photocopying, downloading, broadcasting or electronic transmission, without prior written consent of Aon Corporation.

Trademarks

owned by Aon Corporation, or third parties who have authorized their use.

Nothing contained on this presentation should be construed as granting any license or right to use any Mark displayed in the presentation without the written permission of Aon Corporation or such third party that may own the Mark. Misuse of any Marks, or any other content, displayed on this website is prohibited.

The trademarks, service marks, trade names, and logos ("Marks") associated with this presentation are