

Cyber Awareness Webinar

Bronson Justus – Baptist Insurance Services
Chadd Reynolds – Emergence



AGENDA

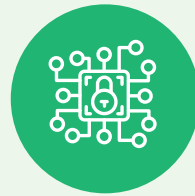
What are we talking about?

Introduction



- Terminology
- Who commits cyber attacks
- Importance

Cyber Risks



- Schools
- Church Groups
- Aged Care
- Baptist Camps

Insurance Covers



- Losses to your Business
- Losses to others
- Cyber Event Response Costs
- Cyber theft

Risk Controls



- Employee training
- Multi-Factor Authentication
- Patching & Updates
- Back-ups
- Funds transfer controls

Cyber events



- System Failure
- Ransomware
- Email compromise
- Social Engineering

Who, What and Why?

Common Terminology:

- Cyber Event
- Threat Actor
- Phishing

Who are the threat actors?

- Motivation to attack

Why is cyber important?

- Risk transfer (and stress transfer)
- Obligations, Notifiable Data Breaches



Key constituent concerns



Education

- Personal Information
- Significant IT infrastructure
- Loss of Funds



Church Ops

- Personal Sensitive Information
- Reputational Harm
- Loss of Funds



Aged Care

- Significant IT Infrastructure
- Compromised Services
- Loss of Funds



Baptist Camps

- Interruption to host camps
- Reputational Harm
- Loss of Funds

What does Insurance provide?

- ✓ Losses To Your Business
- ✓ Liability to Others (incl defense costs)
- ✓ Cyber Event Response Costs
- ✓ Optional – Cyber Crime



RISK CONTROLS

How can you protect your operations?



Employee Training

70% of cyber events have a human element!



MFA

Multi-Factor Authentication – second layer of defense against stolen credentials



Patching

Keep systems patched, apply updates in a timely manner.



Backup

Limit potential for ransom payments.

Secure funds transfers

- Theft of funds is consistent, ongoing threat.
- Social Engineering has lower bar to entry for criminals
- Process-driven, free protections:
 - Employee Awareness Training
 - Enforce Multi-Factor Authentication
 - Double-verify Bank Details
 - Sign-off controls for larger transactions
- Do not rely solely on bank fraud protection



What we are seeing

System Failure



- CrowdStrike

Ransomware



- Not just news headlines
- RaaS
- Double-extortion

Email Compromise



- Common and damaging
- Reused credentials
- Targeted phishing

Social Engineering



- No technical expertise
- Need to fool someone once
- Increasing AI use

THANK YOU

Q&A

—