INTERCHARGE

RISK MANAGEMENT PRESENTATION FOR MEDICAL PRACTICES & DOCTORS

INTERCHARGE

- 30 + Years in risk solutions for medical practices
- We represent hundreds of doctors + practices and medical colleges
- There will be a test & prizes later ….so pay attention!
- Questions are welcomed at any time

BROKER EXPERIENCE

- We diagnose risk
- We refer our findings to the specialists in the practice
- Years ago an insurance crisis occurred and it changed the insurance industry for Doctors

MALPRACTICE & MEDICAL INDEMNITY

- Medical Indemnity is ‘designed’ for the ‘sole trader’ Doctors
- Are staff employed by the Doctor, or the practice?
- Practice entities generally need their own Malpractice
- Walk in walk out - Is it Public Liability or Malpractice?
- As a broker we help Doctors and the practice managers coordinate & bulk buy insurance to bring the cost down.

INSURANCE PITFALLS

- Cool rooms- 1% of undisclosed EPS could potentially forfeit your insurance policy
- Cold Storage & Stock – the deterioration risk
- Claims made policies – the 'Oh S**T' moment
- Patients switch between public & private, where did the fault begin?
- Employment claims are now 1,000% higher than they were 10 years ago

CYBER RISKS

FOR MEDICAL PRACTICES

INTRODUCTION

- Claims
- How bad is it ?
- Losses
- Prevention
- Protection

CLAIM EXAMPLE 1: MIAMI FAMILY MEDICAL CENTRE

- Staff arrived Sunday morning
- Systems did not operate
- Server screen was locked and a message demanded $4,000
- Business had antivirus, passwords and off site back ups

CONT.

- Hack determined to have originated in Russia
- Used a sophisticated code to encrypt files and the back ups over a period of time
- The practice was able to recover all data **except** the last 12 months

HOW BAD IS IT REALLY: VERIZON MARKET REPORT

- Estimated that 1 in 5 businesses will be subjected to an attack in 2017
- Estimates from industry experts believe Cybercrime is now a $1.65 billion dollar business in Australia alone
- Estimated 38% of all data stolen is medical in nature
- Cybercrime is now officially the highest ranking risk faced by businesses
- Cybercrime is the top item agenda for federal government and ASIC
- The largest bank in Australia is estimated to be attacked 40,000 times a minute

SMALL BUSINESS

- Attacks are targeted at SMEs - they typically have less security measures
- Viruses, malware and ransomware attacks are the most common form of attack
- These types of incidents result in IT expenses and restoration costs to repair systems, and loss of revenue

MARKET DATA

- 15% of the trillions of emails sent are spam/viruses
- A unique malware is created every second
- One in every 82 emails is a phishing attack
- Over 19,000 malicious websites are identified daily
- The average time before a virus is detected is 140 days (Server & Backups)

THE EXPOSURES

- Cyber Extortion
- Point of Sale
- Web Application
- Insider misuse
- Physical Theft (Laptops etc.)
- Errors
- Crimeware
- Card Skimmers
- Denial of Service
- Cyber – Espionage

BLACK HATS / THE DARK WEB

- Infection spreading service = $100 per 1000 Installs
- Denial of service = $535 for 5 hours a day for 1 week
- Exploit kits = $1,000-$2,000
- Credit Card = $1 per C/C number & $10 with the Pin
- Botnet = $700

I/WE ARE NOT A TARGET

Hackers and automated cyber software search through millions of IP addresses all over the world for any kind of access. Once inside via any kind of weakness they can access your system and even stay there without you knowing for months, or even years

CLAIM EXAMPLE 2: EYE SURGERY

- $10+ Million turnover
- Employee opened an email attachment with a virus
- Russian hackers demanded thousands via bitcoin payment
- System was paperless and the clinic struggled to function
- $90,000 in I.T expenses, damages and lost man hours

CLAIM EXAMPLE 3: DISTRIBUTE I.T

- $50,000,000 business
- 30+ staff – each one an expert in I.T
- Attacked 11th June 2014
- Assets liquidated 23rd June 2014
- Perpetrator caught – truck driver
- Police found evidence of 300 other targets

LOSSES FROM A CYBER ATTACK WITH DATA BREACH

- Each patient must be contacted in writing (1 client = 1 letter = $1.00)
- Loss of revenue resulting from downtime
- Data breach of patient information can mean $340K fines for individuals & $1.7M for companies
- Costs of the event response team & I.T Forensic experts to resolve the attack.
- Direct legal action by patients affected
- Losses in restoring data / Payment of ransoms

PREVENTION

- Ensure software is up to date
- Password protection: Use a real one….
- Top 6 Passwords hackers/automated cyber software will start with:

✓123456 12345 Password

✓Default Qwerty Abc123

- Be Smart about USB ports and portable devices
- Never open suspicious emails or media posts

INSURANCE: PROTECTION AGAINST A CYBER FIRE

- It is common for a business to insure against fire, but they are rarer than cyber attacks – Digital FIRE
- 5 years ago cyber insurance would have cost you $15,000
- In 2017 for a small practice it will likely cost you $1,000 depending on the risk profile
- Cover has evolved after examination of over 100,000 events
- Triage with email and phone notification 24/7
- Assessment (review and mitigation)
- Management (deployment of experts)
- Settlement (covering costs and lost revenue)

INSURANCE – TIME FOR A FRANK DISCUSSION

- Grudge purchase
- As Brokers we work with you
- We provide the information for you to make an 'informed decision'
- If you don't ask, or don't listen, the consequences can be ruinous
- It is still a soft market, so don't get stuck in the 'quick renewal' category

TEST & Q&A

Please feel free to ask any questions now

or come and see us after the presentation

Otherwise please feel free to call an Intercharge Risk Advisor

Office: 02 9868 8444

Insurance@Intercharge.com.au