HACKED:
Data Breach Scenario

John McCabe

SVP & Chief Operating Officer, Liberty International Underwriters

Andrew Methven

Risk & Assurance Manager, City of Sydney

Joe Perricone

Experienced Chief Information Officer

Tony Harb

Facilitator

Remember

- Be prepared (plan) vs. “she’ll be right”
- Incident -vs- Crisis -vs- Disaster
- Critical success factors:
  - Situational awareness
  - Prioritisation
  - Leadership
  - Communication

Cyber Incident Response

Security Incidents

- Malware (Virus, Trojan etc)
- Inappropriate or unauthorized access to or use of information
- Unauthorised destruction or modification of data
- Unauthorised disclosure of information classified as Confidential, espionage
- Attempted intrusion of networks or systems
- A Denial of Service (DoS) attack

Scenario Assumptions

- XYZ Ltd – A large service organisation – 250+ people.
- City/CBD location. B grade building…average security.
- The corporate bankers are Eastpac Bank.
- Several large departments – finance, admin, HR, IT, sales etc.
- Highly automated business processes. Use MYOB for all accounting and payroll.
- High volumes of credit card sales, direct debit transfers and direct debit supplier payments.
- Stakeholders require privacy of information.

10:00
Tuesday 28th October

- You receive an email from your CEO to advise that:

  3 laptops were stolen overnight. One from finance, one from HR and one from marketing…please remember it is company policy to take your laptops with you or lock them up each night, failure to comply with this policy will result in instant dismissal.

  Sincerely,

  CEO, XYZ Ltd

  Anything else you want to know?

  Any concerns at this stage?

13:00
Tuesday 28th October

- You receive a call from the CFO to say that she has just received a call from Eastpac Bank advising her that the banks Fraud & Suspicious Transaction Unit has identified 10 authorised transactions (transfer payments) for $49,999 each on your bank account to a bank account in China. As per Eastpac Bank policy, the transactions were not completed pending authorisation. She has declined approval, but asks you what she should do now…as it may happen again?

What do you suggest?

09:30
Wednesday 29th October

- Reception/customer service contact you to advise that 3 customers called in just the last 15 minutes querying transactions appearing on their credit cards ranging from $750 to $1,300. The customers did not owe money.
- You check with Finance and there is no corresponding credit in our bank statement for the transaction.

What do you do?

11:30
Wednesday 29th October

- A reporter from the Sydney Morning Herald calls wanting to know how private information relating to XYZ Ltd's customer credit cards was leaked and if you are going to compensate them?

What do you say?

When do you communicate?

Who communicates?

Is there insurance cover?

14:30pm
Wednesday 29th October

- An article relating to the unauthorized credit card transactions data breach appears in the on-line version of Sydney Morning Herald.

What do you do?

Does your media response strategy change?

15:30
Wednesday 29th October

- The CFO receives an auto generated email from the web-based MYOB system advising that her password has successfully been reset. However, she did not perform a reset.
- She reports it to the help desk immediately. User access log monitoring by the help desk identify that the CFO's User Id is currently updating the supplier master file and performing banking transactions. The transactions were requisitioned by an unknown user id.

What steps should the organisation take now?

What are the priorities?