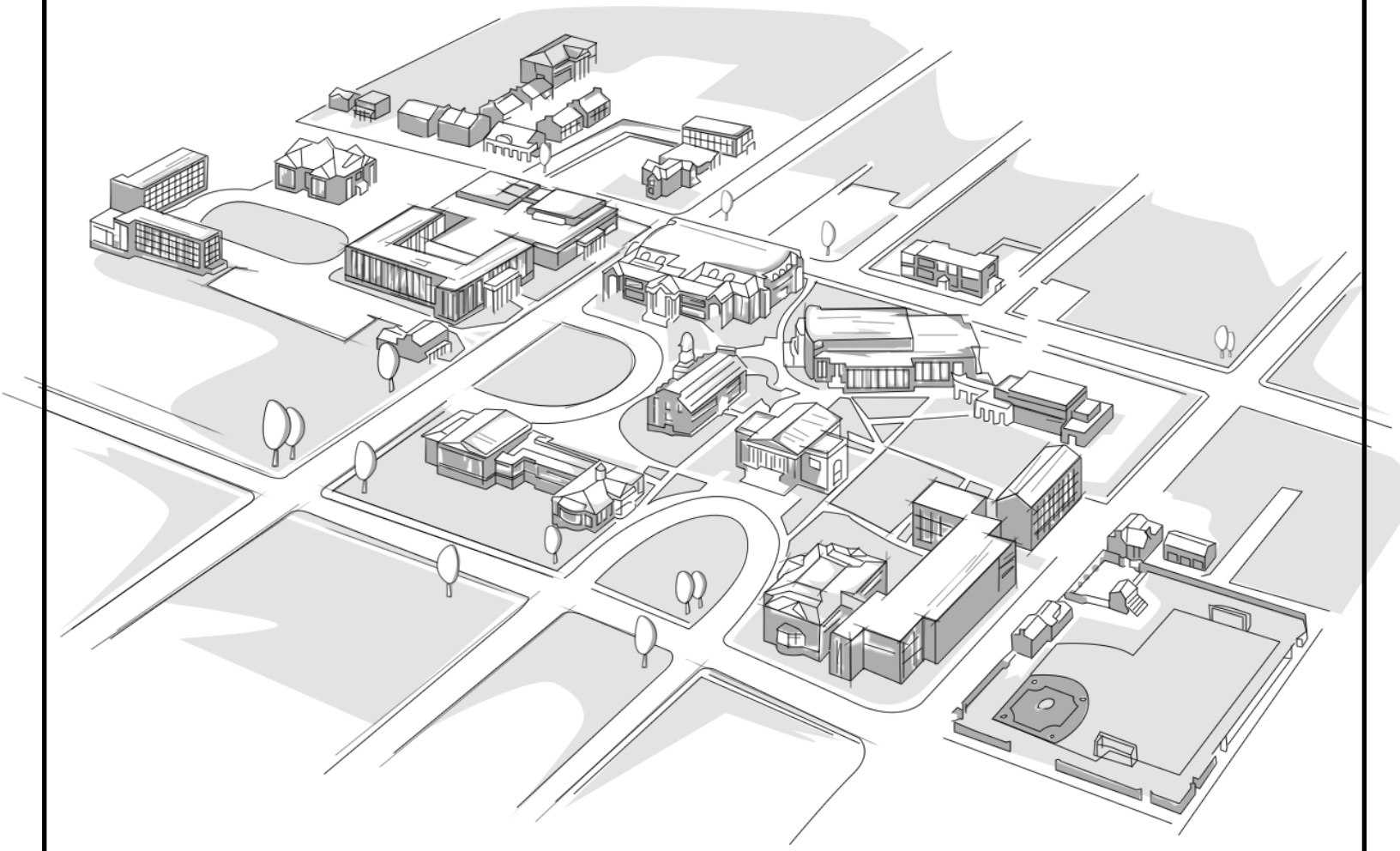
BROOKLYN

CYBER LIABILITY

Lecturer: Freddie Arguelles



CYBER PROTECTION PRESENTATION

BROOKLYN

BROOKLYN UNIVERSITY

WHAT IS A CYBER ATTACK?

BROOKLYN

- An attempt to damage, disrupt or gain unauthorised access to a computer, computer system or electronic communication network
- In the last 20 years, cyber attacks have evolved from simple ‘pop-up’ ads to a complex illegal economy
- In 2013, over three billion records were ‘lost’. 74% from the USA
- Various industries have been the victims including retail and technology business, financial service providers and goverments.

BROOKLYN UNIVERSITY

CYBER ATTACKS IN AUSTRALIA

BROOKLYN

- While Australia has not witnessed the severity of attacks seen in the USA, the number is on the rise.
- In 2014 it is estimated Australia's Cyber attacks rose by 20%!

Cyber attacks on Australian businesses rose 20pc last year

By business reporter Emily Stewart

Updated 24 Apr 2015, 9:00am

Cyber attacks on Australian businesses and government increased by 20 per cent last year, according to a defence force intelligence unit.

The Australian Signals Directorate said the most commonly targeted sectors are banking and finance, resources and energy, defence capability and telecommunications.

"It's an arms race - it's a cyber arms race - where sometimes the bad guys will get a little bit ahead and sometimes the good guys will get a little bit ahead," said IT security consultant Wade Alcorn.

VIDEO: Government figures suggest a 20 per cent rise in cyber crime last year (The Business)

MAP: Australia

The Commonwealth Bank, the country's biggest bank, receives millions of cyber attacks daily from organised crime and so-called 'hactivists' - people using hacking to further a social agenda.

According to CBA's chief of information security, Ben Heyes, the number of serious attacks are rapidly on the rise.

"We're seeing the tools that are available for executing a cyber attack are becoming more widespread and becoming increasingly more sophisticated and, with that, we're seeing a large increase in the volume of attacks," he observed.

"We have categories of attacks that are designed to disrupt services and there are categories of attacks that are designed to gain access to an organisation's internal environment - to potentially withdraw from that intellectual property or data that's important."

BROOKLYN UNIVERSITY

SOME GLOBAL CURRENT STATISTICS

BROOKLYN

- 91% increase in targeted cyber attacks in 2013*
- 62% increase in the number of breaches in 2013*
- 31% of all targeted attacks against businesses with fewer than 250 employees*
- 60% of small businesses have suffered a malicious breach in the past 12 months alone*
- 24% of companies surveyed report they have been a victim of cybercrime**

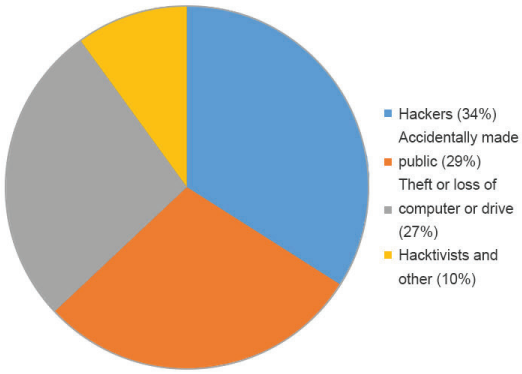
*Symantec Internet Security Threat Report 2014

**PWC 2014 Global Economic Crime Survey

BROOKLYN UNIVERSITY

TOP CAUSES OF DATA BREACH IN 2013

BROOKLYN



Symantec Internet Security Threat Report 2014

BROOKLYN UNIVERSITY

COSTS OF CYBER ATTACKS TO THE ECONOMY IN 2013

BROOKLYN

- In 2013, the estimated cost of cyber related hacks on the global economy was $445billion.
- In Australia the estimated cost to the economy was $1.06billion.
- The largest reported single was $58 million.
- The average cost per affected business in the USA was $11.06million
- In Australia the average cost per business was $3.67million
- The total number of Australian victims was just over 5 million
- The average cost per [affected] person was $201

2013 Norton Report, Symantec and Ponemon Institute 2013 Research Report

BROOKLYN UNIVERSITY

METHODS OF CYBER-ATTACK DELIVERY

BROOKLYN

Phishing emails

- A wide net is cast to many random individuals

e.g. unsolicited emails

Spear phishing

- Targeted phishing emails to individuals Illegitimate websites

Illegitimate websites

- Often accessed via the phishing email link

Advertisements

- Banner ads, pop-ups etc

Downloads and plug-ins

- Deliberate download by the individual not knowing of the attack / virus

Denial of Service attacks

- Websites and systems accessed and controlled remotely

BROOKLYN UNIVERSITY

MOTIVES AND TYPE OF INCIDENTS?

BROOKLYN

- Competitor seeking a commercial advantage
- Malicious damage
- Using the system for further attacks
- Personal grievance
- Issue motivation/hacktivism

- Other (including carelessness, lack of attention, negligence)
- Illicit financial gain
- Random or indiscriminate – for example hackers! Who generally do not discriminate. The National leader of a large international broking firm recently confirmed this, advising hackers often will simply "scan networks indiscriminately, looking for vulnerabilities without a specific target"

Cyber Crime & Security Survey Report 2013 CERT Australia

BROOKLYN UNIVERSITY

ENTERPRISE RISK MANAGEMENT

BROOKLYN

The following 'Enterprise Risks' demonstrate the risks faced by the average Australia business from their staff profile, in 2013:

- 33% use the same password for both work and personal devices
- 35% have clicked on a link from an unknown sender
- 58% have sensitive information on their mobile devices
- 59% store work information in the Cloud.
- 30% leave mobile devices unattended in their vehicle

Cyber Crime & Security Survey Report 2013, CERT Australia

BROOKLYN UNIVERSITY

HOW TO PREVENT A CYBER ATTACK?

BROOKLYN

A well developed risk management policy will cover the following:

1. Network protection
2. Data inventory
3. Incident response
4. Security policies and plans
5. Encryption requirements
6. Password policies and procedures
7. Privacy and data management
8. Disaster recovery
9. Intrusion detection and data loss prevention

For large organisations, the risk management program may involve coordinating the risk management dept, IT team, corporate trainers and external auditors.

BROOKLYN UNIVERSITY

STEPS IN RISK MANAGEMENT 1

BROOKLYN

- Use strong passwords and change them regularly (do not use vendor supplied defaults for system passwords).
- Screen email attachments and Internet downloads.
- Install, maintain and update anti-virus software.
- Install and use a firewall.
- Remove unused software and user accounts, delete all contents of replaced equipment.
- Establish physical access controls for all IT equipment.
- Back-up important files, folders and software.
- Keep current with software updates (patches).

BROOKLYN UNIVERSITY

STEPS IN RISK MANAGEMENT 2

BROOKLYN

- Review company website for potential liability for content, vulnerabilities and controls.
- Physically inspect network setup, observe operations.
- Implement intrusion detection system.
- Conduct penetration testing – simulate attack. See if intrusion is detected and safeguards work.
- Staff re-training, update policies / procedures.
- Change default settings, remove / disable unnecessary or insecure services, e.g. USB ports of computers.
- Transfer risk through insurance.

BROOKLYN UNIVERSITY

RESPONDING TO DATA BREACHES

BROOKLYN

Step 1 – Contain the breach and conduct a preliminary assessment.

Step 2 – Evaluate the risks associated with the breach.

Step 3 – Notification (Internally, to the OAIC and to police if required).

Step 4 – Prevent further breaches.

BROOKLYN UNIVERSITY

BROOKLYN'S CYBER DATA PROTECT POLICY

BROOKLYN

In the following pages we outline the key covers provided by a current Cyber Liability policy. The example we will use is the Brooklyn Cyber Data Protect Policy. Areas of cover include:

- Security & Privacy Liability
- Multimedia Liability
- Privacy Penalties
- Privacy Response Costs
- Network Asset Protection, including Business Interruption
- Cyber Extortion & Terrorism

BROOKLYN UNIVERSITY

CYBER DATA PROTECT COVERAGE

BROOKLYN

Security & Privacy Liability

Third Party loss resulting from:

- the alteration, copying, corruption, destruction, deletion, or damage to electronic data on a computer system;
- unauthorised disclosure of confidential commercial, corporate, personally identifiable, or private information;
- theft or loss of electronic and non-electronic data which is in the Named Insured's care, custody or control, including data in the custody of outsourcers and independent contractors (provided it is within the scope/course of their employment);
- failure to disclose a breach of security affecting personally identifiable, nonpublic information, or failure to dispose of such information within the required time period in violation of notification laws or regulations in effect now or in the future;
- failure to prevent transmission of malicious code or computer virus from a computer system to third party computers or systems;
- failure to prevent or hinder participation in a denial of service from a computer system operated by the Named Insured or on the Named Insured's behalf directly at internet sites or computer systems of a third party

BROOKLYN UNIVERSITY

BROOKLYN'S CYBER DATA PROTECT POLICY

BROOKLYN

Multimedia Liability

- Defamation
- Invasion of Privacy
- Plagiarism
- Infringement of Copyright, trademark, domain name

BROOKLYN UNIVERSITY

Privacy Regulatory Defence & Penalties

- cover for civil regulatory action, including civil penalty, or fines to the extent insurable by law, imposed by a federal, state, or governmental regulatory body as a result of a privacy breach, security breach, or breach of privacy regulations

Privacy Breach Responses costs, Customer Notification Expenses, and Customer Support and Credit Monitoring Expenses

CYBER DATA PROTECT COVERAGE BROOKLYN

Network Asset Protection

- Damage, alteration, corruption, distortion, theft, misuse or destruction of the insureds own digital assets (data and computer programs, not hardware) resulting from a failure to prevent or hinder any of the following attacks:
    - Denial of Service
    - Malicious Code
    - Unauthorised Access
    - Unauthorised Use
- **Business Interruption**

BROOKLYN UNIVERSITY

CYBER DATA PROTECT COVERAGE

BROOKLYN

- **Cyber Extortion**

  cover for amounts paid in order to fulfil the demands of extortionists who target the insured's digital assets or their customers' private information.

- **Business Interruption**

  business interruption costs that result from disruptions of the insured's computer system caused by acts of cyber terrorism

  - Electronic or digital threat of any person or group(s) of persons, whether acting alone or on behalf of, or in connection with any organisation or government which disrupt the computer system

BROOKLYN UNIVERSITY

CLAIM SCENARIO 1 – LOST HARDWARE

BROOKLYN

- Medium sized accounting firm
- One of your key employees, Jeff, leaves a function where he has been with a number of high profile clients
- Jeff's Laptop is next to the bar, which contains a number of unencrypted files on it, and access to email, with personal information on client's freely available including addresses and bank account details.
- Despite calling the bar and making other inquiries it becomes clear Jeff's laptop is lost for good.
- Costs:

  identifying and notifying all the affected clients, and this may include IT forensic investigations, providing credit monitoring services and if necessary hiring a PR firm to manage any reputational damage.

BROOKLYN UNIVERSITY

CLAIM SCENARIO 2 – BLOG/FORUM

BROOKLYN

- After some solid years of growth and building an extensive client list, you decide that it is time for your engineering firm to set up a blog in order to help educate your clients and keep them up to date with current trends.
- A well qualified engineer posts an article taken from company PKL, regarding a new technique for undertaking structural assessments of existing buildings.
- The article is posted without reference to the source and is also used in some printed marketing materials.
- Your firm receives a cease and desist letter, negotiations with PKL break down and civil proceedings are commenced against your firm.
- Costs:

  - defending the plagiarism/misappropriation of ideas claim.

  - Other costs may include defending claims for infringement of trade marks, breach of copyright, libel/slander, product disparagement and payment of any settlement monies.

BROOKLYN UNIVERSITY

CLAIM SCENARIO 3 – CYBER EXTORTION

BROOKLYN

- Do you hold data?
- You arrive at work one morning and run through your routine, turn on your work computer, go and make your morning coffee.
- When you arrive back at your desk, the screen is blank, except for three sentences written on the screen:

  Your files have been locked and you cannot gain access.
  Pay $25,000 before 30 November 2014 or we will destroy all data.
  Bank Account Details XXXX

- There are many ways a hacker(s) may choose to extort money from a business including the above, a DOS attack, introduction of malicious code etc.
- Costs:

  - payment of monies to restore access (if deemed credible),

  - IT forensic investigation to check all data is ok

  - repair and recovery of data.

BROOKLYN UNIVERSITY

CLAIM SCENARIO 4 – PHISHING (DO YOU USE EMAIL?)

BROOKLYN

- Several team members from an architectural firm receive emails claiming to be from the Office of State Revenue regarding an outstanding penalty payment.
- The business manager who happens to be curious, opens the email in Outlook, clicks the link and then quickly deletes the email and closes Internet Explorer.
- Shortly after clicking the link files and programs start deleting from the company's computer system.
- Internal IT does testing, confirms the cause of the issue was a virus that was released through the email.
- Due to the continuing deletion of files/programs the company decided to shut down the system and restore from a backup the night before.
- All work, including emails sent and received for 24 hours are lost and the company was offline for a total of 36 hours.
- Costs:
  - IT forensics and data and program restoration,
  - business interruption.

BROOKLYN UNIVERSITY

REFERENCES

BROOKLYN

- Symantec Internet Security Threat Report 2014
- PWC 2014 Global Economic Crime Survey
- Cyber Crime & Security Survey Report 2013, CERT Australia
- www.oaic.gov.au/privacy
- www.cert.gov.au

BROOKLYN UNIVERSITY