FREIGHT TRADE ALLIANCE

SYDNEY 9 APRIL 2019

Jonathan Sharrock CEO – CYBER CITADEL
jonathan.sharrock@cybercitadel.com

00 20 00 2F 00 53 00 54 00 30 20 00

00 64 00 3A 00 25 00 30 00 00 32

00 74 00 20 00 25 36 00 30

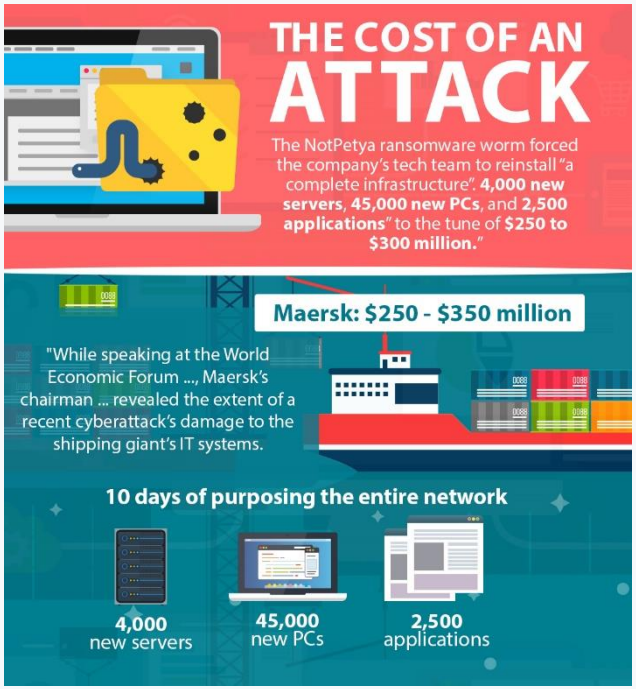
YOU ARE TARGETED!

00 30 00 32 00 64 2E 00 20

00 00 00 73 00 68 00 78 00 52 74 00

00 6E 00 2E 00 65 00 78 00 79 65 00

MAERSK IN THEIR 2017 NOTPETYA ATTACK



- Had 10 working days dark
- Admitted it cost them $250-$300 Million (lowball)
- Replaced 14,000 servers, 45,000 PCs and 25,000 new applications

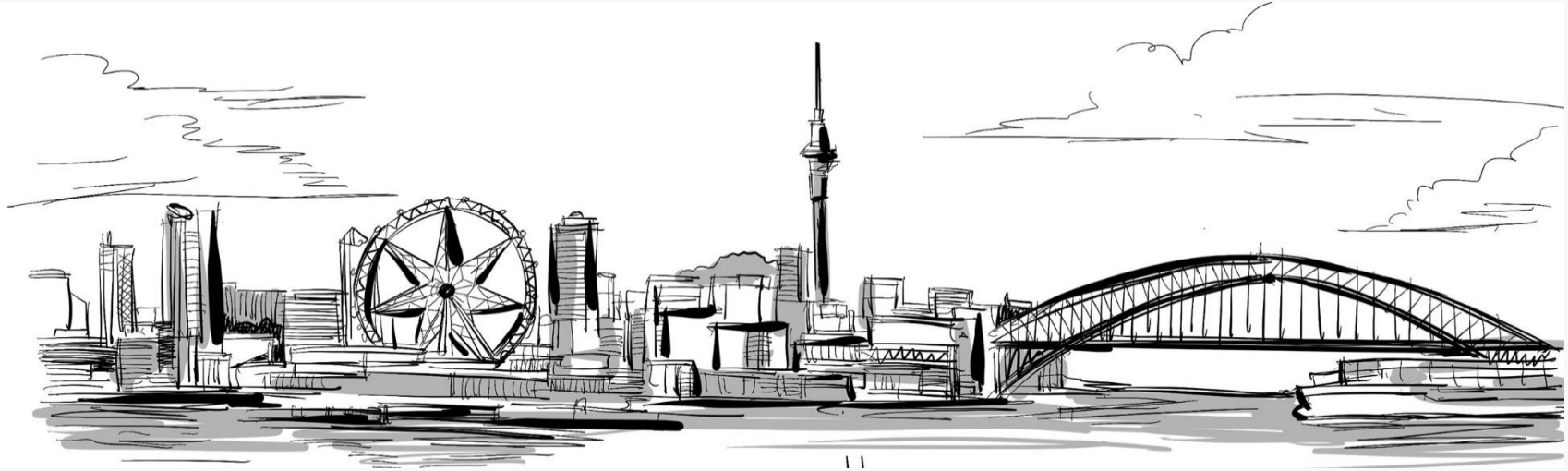
BUT THIS WAS THE TIP OF THE ICEBERG FOR THEIR SUPPLY CHAIN…

- Merck claimed a $870 million loss
- TNT Express reported a $400 million loss
- French construction giant Saint-Gobain lost around the same amount
- Reckitt Benckiser, Cadbury
- Only the public companies

IN 2019 CYBER SECURITY MATTERS

- Your customers need to feel protected
- Not only that, you are required to do so by law
- There are many regulations around this
- If you are dealing in international logistics, then multiple countries' laws may be applicable to them
- In the event that a cyber attack happens, you may fend off would-be lawsuits by showing that you had taken adequate measures for security

WHO ARE WE?



SYDNEY / MELBOURNE / AUCKLAND

PENETRATION TESTING & VULNERABILITY ASSESSMENT

INCIDENT RESPONSE

CONSULTING

AUSTRALIAN MANDATORY DATA BREACH REPORTING REQUIREMENTS

Who do they apply to?

Any business that turns over $3m AUD per year

And, some that don't

- If you hold financial / credit or health information
- You are part of a bigger group
- Have been told to

AUSTRALIAN MANDATORY DATA BREACH REPORTING

WHAT IS AN ELIGIBLE DATA BREACH?

- Loss of personal information – company laptop, phone, USB stick
- Unauthorised access of personal information – malware, ransomware, malicious attack, email sent to the wrong people, hacking or any unauthorised access (past employee)
- Loss or unauthorised access that a reasonable person (person in charge of information CIO, CFO, security personnel) believes could cause serious harm

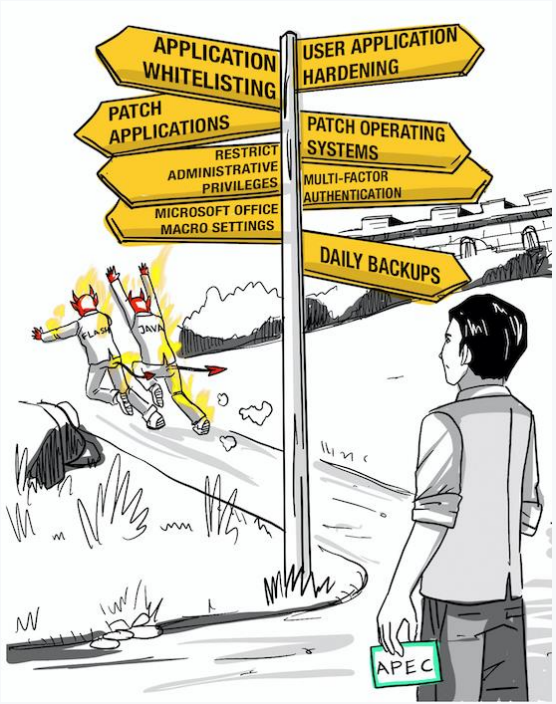
WHAT ARE THE CONSEQUENCES IF YOU DON'T?

Fines:	Up to $2.1 million for corporations, $420,000 for individuals
	Up to $2.1 million pecuniary fine for corporations for a repeated serious offence
Determinations:	Can require an apology, or pay damages to affected individuals, pay the individual's costs, undertake specific training, or take other specified action
Enforceable undertakings:	Be instructed what to be, e.g. security audit and compliance

PREVENTION

FOLLOW THE ESSENTIAL 8 MITIGATION STRATEGIES

1 – 4 PREVENT MALWARE



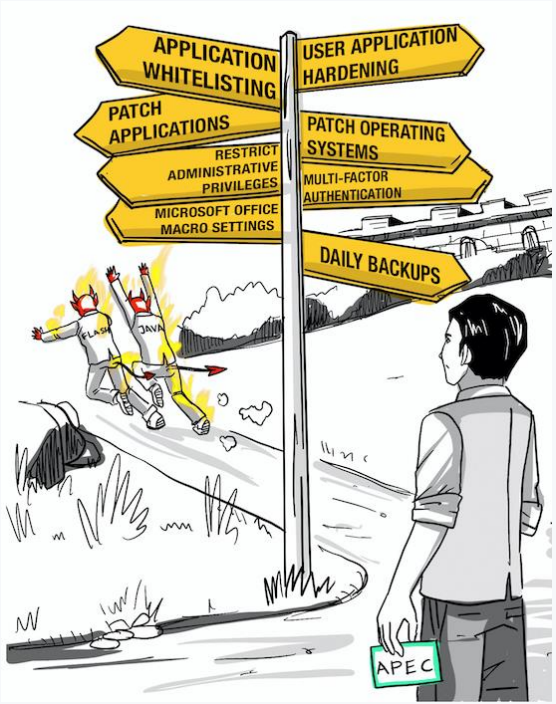
01 **USE WHITELISTS**

02 **PATCH APPLICATIONS**

03 **BLOCK MACRO USE IN MICROSOFT OFFICE**

04 **USER APPLICATION HARDENING**

5 – 7 LIMIT THE EXTENT OF CYBER SECURITY INCIDENTS

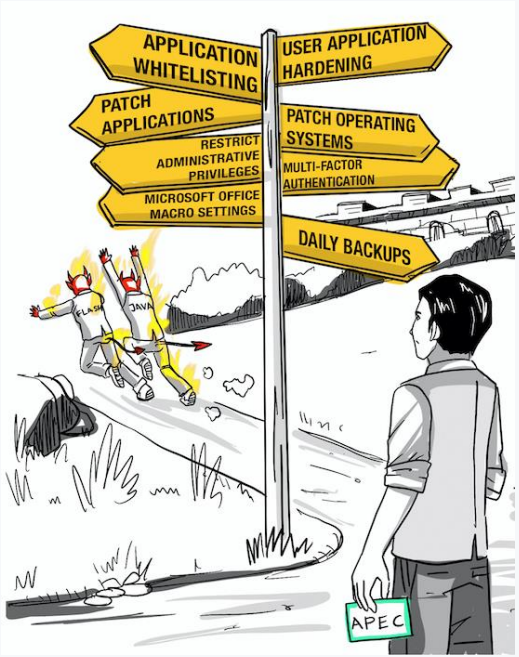


05 **RESTRICT ADMINISTRATIVE PRIVILEGES**

06 **PATCH OPERATING SYSTEMS**

07 **MULTI-FACTOR AUTHENTICATION**

8 MITIGATION STRATEGIES TO RECOVER DATA AND SYSTEM AVAILABILITY



08 **DAILY BACKUPS**

Important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.

ACCESSING THE INTEGRATED CARGO SYSTEM USE MUST USE DIGITAL CERTIFICATE

Three types

1. Company with ABN Number
2. Company without ABN Number (foreign)
3. Individual

- If you want to use software to send EDI messages, you must use a Device Certificate
- If for multiple people you must have one Certificate Manager
- You must have a certificate for every user of the system
- Letting other people use the certificate is fraud

THANK YOU