Grant Thornton

An instinct for growth™

IT governance: the key to preventing and limiting IT fraud

Matt Green and John Picot
Partner, Technology Advisory & Solutions
Grant Thornton Australia

Agenda

Today we will take a workshop approach to IT fraud and security.

We look at the drivers for fraud and changes that put aged care at risk.

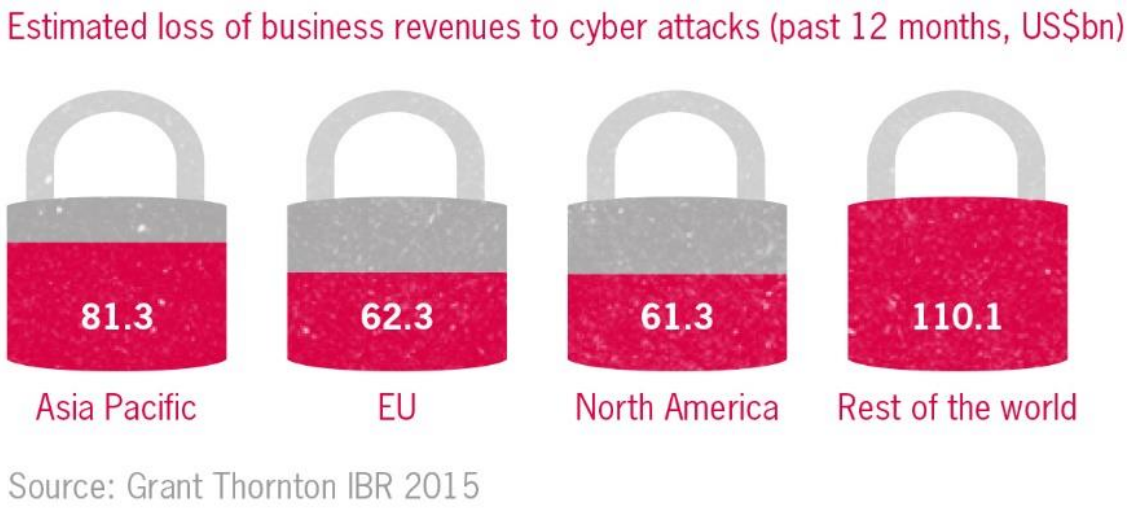
Matthew Green
Partner – Technology
Growth Advisory
Grant Thornton Australia

So to focus our minds we will unpack some recent case studies and discuss governance strategies that would change the outcome.

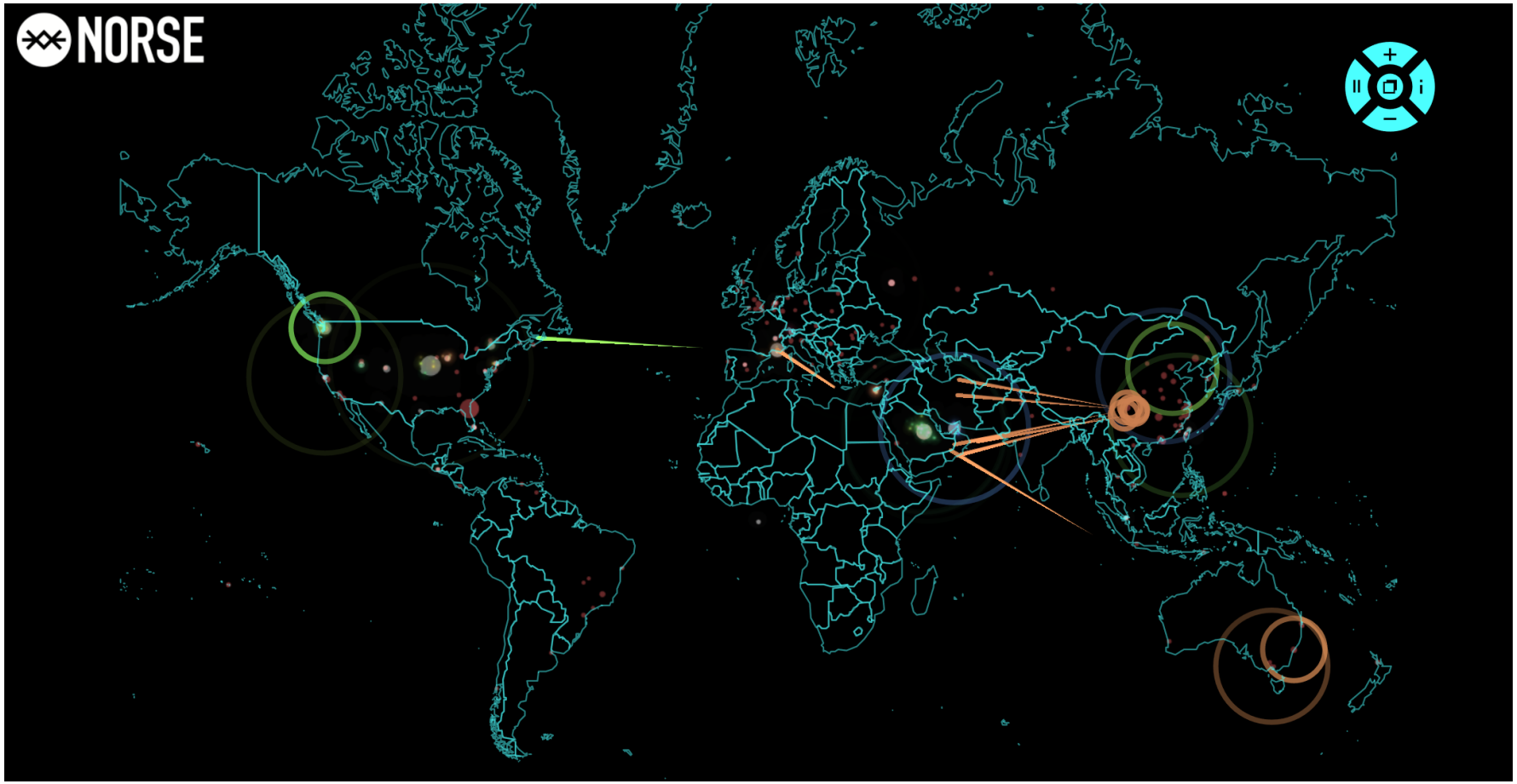
John Picot
Principal - Health and Aged Care
Growth Advisory
Grant Thornton Australia

Why all the focus on cyber security?

- Recent events which have been very public
- Convergence: we ‘live’ in the cloud or ‘on’ the internet
- Hacking is costly
- Statistics are compelling
- Increasing interest from Government and Regulatory bodies



Let's see what's happening right now

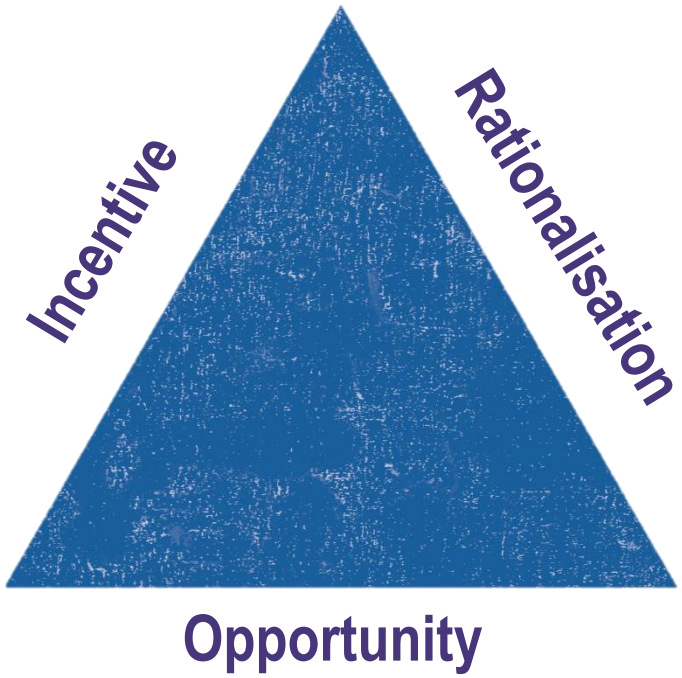


Stopping the hackers is enough, right?

- External hackers are a big threat
- Internal failures are just as big a risk
- Security is a supply chain issue
  - People
  - Process
  - Technology

Why & when does fraud happen? - Fraud triangle

Fraud can be committed if a person is presented with a certain combination of circumstances. This is explained by the **"Fraud Triangle"**



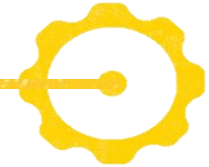
Sector change…

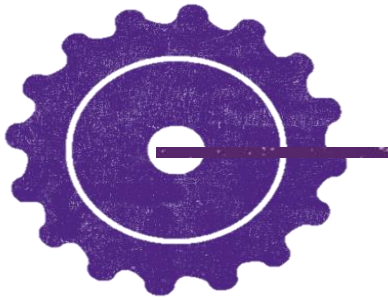
- Government trend to activity based funding with health, aged care and disability leading the way
- Moving from one customer to many
- Transactions increase in volume exponentially
- Transactions decrease in size dramatically
- With increasing service scale, data volumes grow
- Prospects as well as customer information now in the mix
- Competition driving greater digital presence and vulnerability
- Mobility solutions open new access to data
- Opportunity for fraud increases with transaction volumes, data richness, increased channels and digital presence

What should you do about it?

- The historic approach of prevention is no longer valid.
- The board's approach needs to change to a posture of preparedness and proactive response:
  - balancing focus on people, process and tools to help them get ahead of cybercrime
  - The company's board should set the tone for enhancing security and determine who should have oversight responsibility.

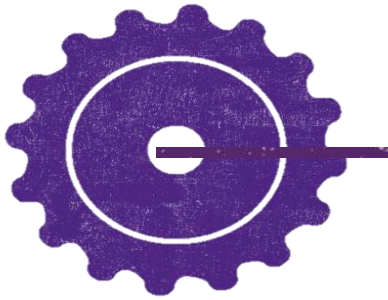
- The current climate calls for a multi layer approach
  - **Identify** the real risks
  - **Protect** the most important information
  - **Sustain** though governance and compliance
  - **Improve** to move with the rapid changes





Anonymous questions about your devices…

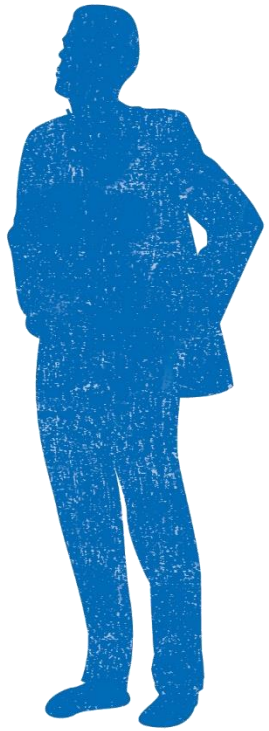
- Who today is using the 'free' conference Wi-Fi?
- Who is using the Wi-Fi to access corporate information?
- Are you using two factor authentication?
- Who has sensitive data stored directly on the device with them today?
- Is your device encrypted?
- Would you know what to do if you lost your device?



Case Study 1

Sydney University

Sydney University 'lost' computer containing sensitive student information



The University …..has admitted it "lost" a notebook computer containing sensitive information about students using disability support services, in a major privacy breach that has shocked and angered students.

As the Baird government is urged to tackle privacy law reform, the university warned on Friday it could not "absolutely guarantee the security" of a confidential database containing students' names, dates of birth, contact details and disability diagnoses.

A notebook computer containing the Disability Assist Database was "lost in transit" on Monday night, students were told in an email. While the computer was password protected, it was "possible that the database could be inappropriately and unlawfully accessed".

Sydney Morning Herald March 2016

Case Study 2

What are the failings in this case?
How could each be prevented?
What are the responsibilities at each tier of the org. structure?

Case Study 2

Red Cross

Red Cross Blood Service admits to personal data breach affecting half a million donors

The personal data of 550,000 blood donors that includes information about "at-risk sexual behaviour" has been leaked from the Red Cross Blood Service in what has been described as Australia's largest security breach.

Data from blood donor registration form posted insecurely online.

Leak included identifying information and "personal details" of 550,000 donors.

The organisation said it was told on Wednesday that a file containing donor information was placed on an "insecure computer environment" and "accessed by an unauthorised person".

The file contained the information of blood donors from between 2010 and 2016.

ABC News 28 Oct 2016

Case Study 2

What are the failings in this case?
How could each be prevented?
What are the responsibilities at each tier of the org. structure?

Case Study 3

Big W

Big W shutters online shopping after data leak

Retailer Big W's website remains in browsing-only mode after a glitch meant shoppers were shown the personal information of other customers.

In a notice to customers, Big W said the "technical issue" occurred on Thursday November 10 between 1.50pm and 3pm.

It meant "the first stage of the checkout process [was] pre-populated with the personal information of another customer".

The data leak included a customer's name, phone and address.

Big W took down the website at 3pm on Thursday, and it has remained in browse-only mode since.

IT News Nov 13 2016

Case Study 3

What are the failings in this case?
How could each be prevented?
What are the responsibilities at each tier of the org. structure?

Governance – who is responsible?

Ask the right questions…

Certain of approach

Priority, principles and process

Informed and vigilant

For more information please contact

Matthew Green
Partner - Technology
Growth Advisory
Grant Thornton Australia
0414 795 982
matthew.green@au.gt.com

John Picot
Principal – Health and Aged Care
Grant Thornton Australia
0434 392 435
john.picot@au.gt.com

Grant Thornton | An instinct for growth™