Data Governance

A framework for Community Legal Centres

Presented by Richard Berkahn and Reece Corbett-Wilkins
Senior Associates from Clyde & Co

27 August 2020

Community Legal Centres Queensland

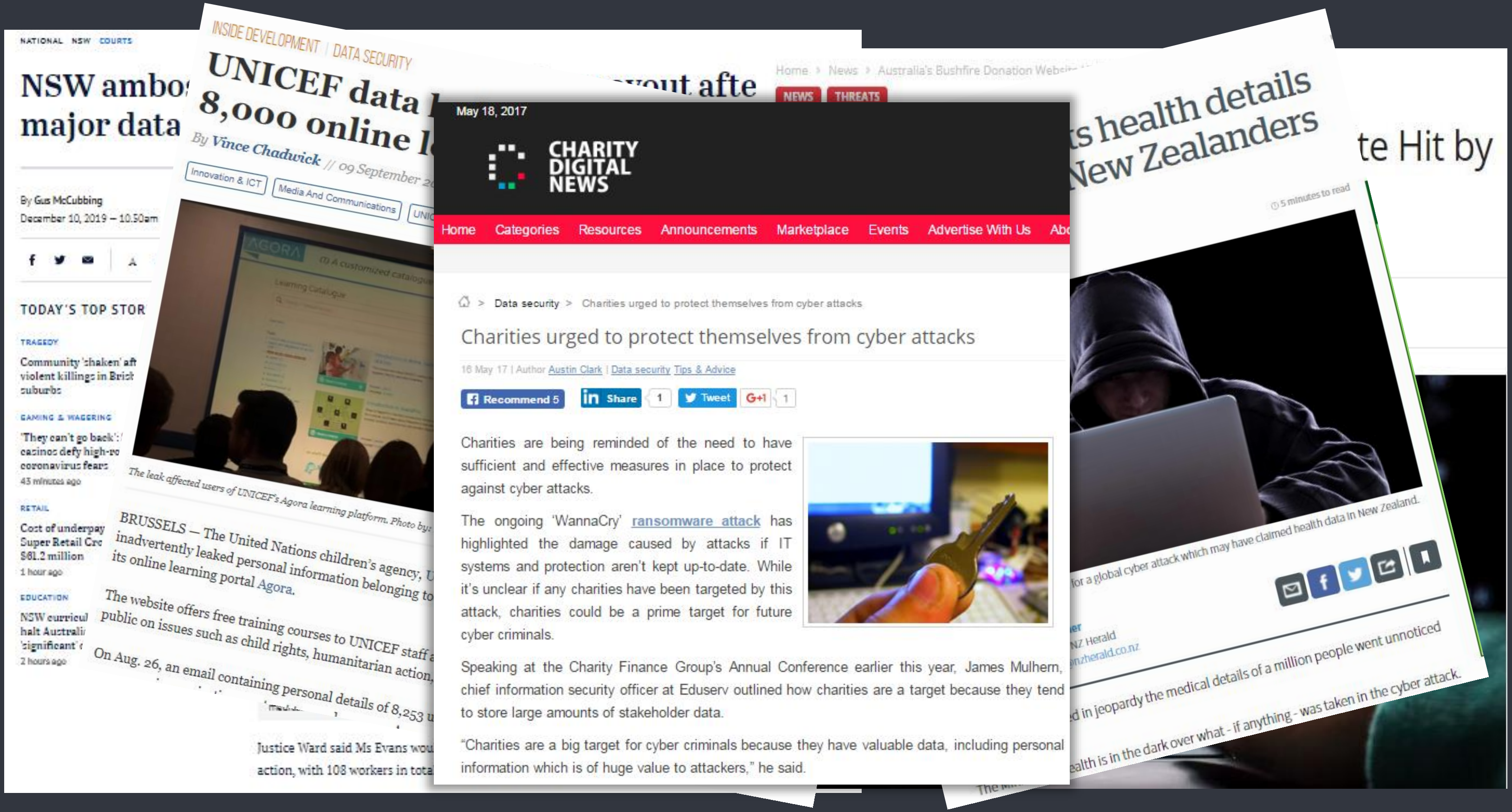
Introduction

What we will cover

- Introduction to ‘data’ and the cyber landscape
- Data Governance – what is it and why is it important?
- A framework for strong Data Governance with some best practice tips
- Questions

Today’s webinar is legal information only, not advice**

Introduction



NATIONAL NSW COURTS

NSW ambo
major data

By Gus McCubbing
December 10, 2019 — 10.50am

TODAY'S TOP STOR

TRAGEDY
Community 'shaken' aft
violent killings in Brisb
suburbs

GAMING & WAGERING
'They can't go back':
casinos defy high-ro
coronavirus fears
43 minutes ago

RETAIL
Cost of underpay
Super Retail Gro
$61.2 million
1 hour ago

EDUCATION
NSW curricul
halt Australi
'significant'
2 hours ago

Justice Ward said Ms Evans wou
action, with 108 workers in tota

INSIDE DEVELOPMENT | DATA SECURITY

UNICEF data
8,000 online l

By Vince Chadwick // 09 September 2

Innovation & ICT | Media And Communications | UNIC

The leak affected users of UNICEF's Agora learning platform. Photo by:

BRUSSELS — The United Nations children's agency, U
inadvertently leaked personal information belonging to
its online learning portal Agora.

The website offers free training courses to UNICEF staff a
public on issues such as child rights, humanitarian action,

On Aug. 26, an email containing personal details of 8,253 u

yout afte

Home › News › Australia's Bushfire Donation Websi

NEWS THREATS

May 18, 2017

CHARITY DIGITAL NEWS

Home | Categories | Resources | Announcements | Marketplace | Events | Advertise With Us | Abo

Data security > Charities urged to protect themselves from cyber attacks

Charities urged to protect themselves from cyber attacks

16 May 17 | Author Austin Clark | Data security Tips & Advice

Recommend 5 | Share 1 | Tweet | G+1 1

Charities are being reminded of the need to have sufficient and effective measures in place to protect against cyber attacks.

The ongoing 'WannaCry' ransomware attack has highlighted the damage caused by attacks if IT systems and protection aren't kept up-to-date. While it's unclear if any charities have been targeted by this attack, charities could be a prime target for future cyber criminals.

Speaking at the Charity Finance Group's Annual Conference earlier this year, James Mulhern, chief information security officer at Eduserv outlined how charities are a target because they tend to store large amounts of stakeholder data.

"Charities are a big target for cyber criminals because they have valuable data, including personal information which is of huge value to attackers," he said.

s health details
New Zealanders

5 minutes to read

for a global cyber attack which may have claimed health data in New Zealand.

er
NZ Herald
nzherald.co.nz

d in jeopardy the medical details of a million people went unnoticed

ealth is in the dark over what - if anything - was taken in the cyber attack.

The Mi

te Hit by

Introduction to ‘data’ and the cyber landscape

What is data?

How is data collected and why is it collected?

Introduction

Who and what are CLCs collecting data about?

Donors and supporters

Contractors or Consultants

Members of public

Clients or Service Users

Volunteers

Employees

Members

Board

Other organisations

Government

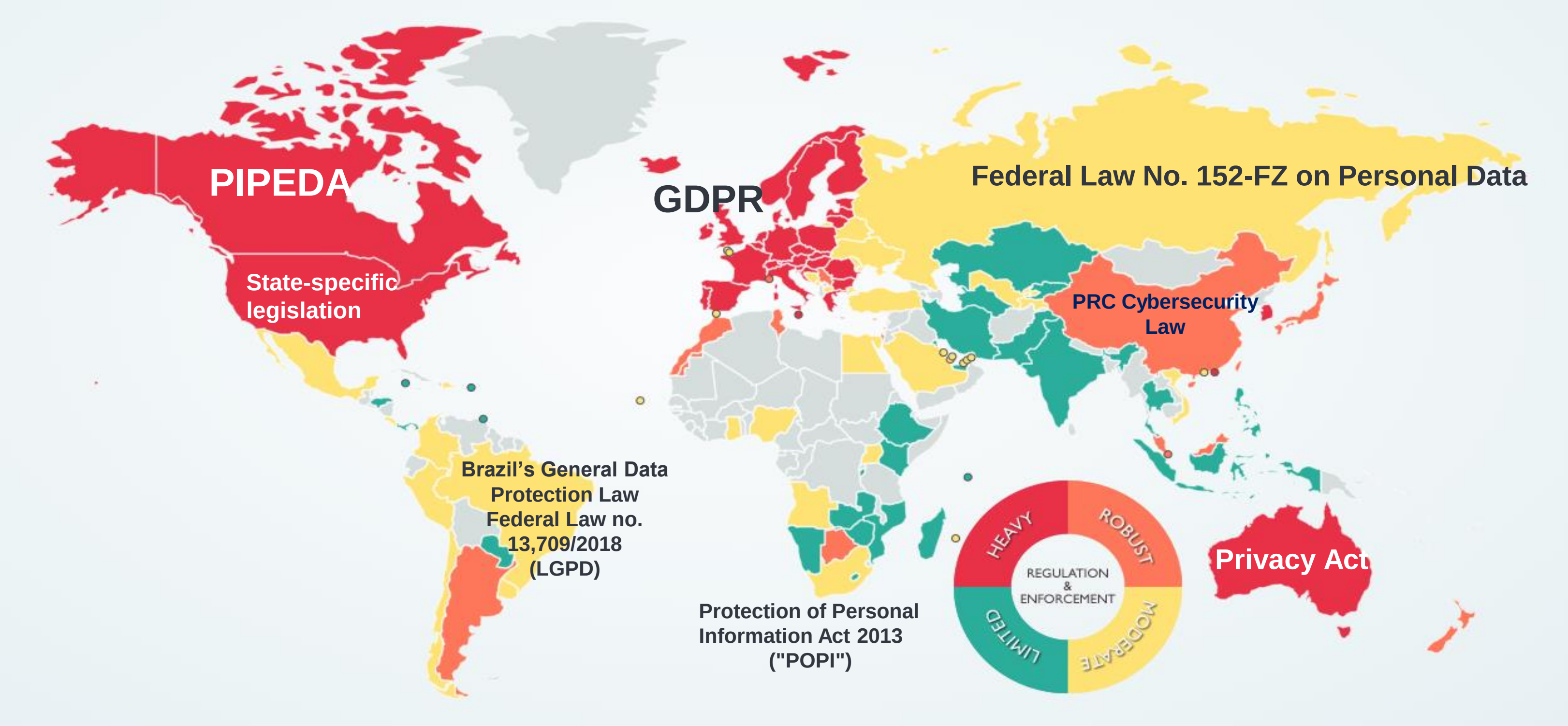
Introduction to ‘data’ and the cyber landscape

Are not-for-profit organisations targeted?

- No organisation is safe: NASA, the most technologically advanced organisation on the planet, was hacked using a $25 computer last June
- Whilst cyber-attacks are typically aimed at commercial businesses, not-for-profit organisations are at risk too:
  - Having personal, sensitive or financial data on servers makes any entity a target
  - Threat actors (‘hackers’) can sell private health data and financial information on the black market
  - Often NFP’s don’t have adequate defence mechanisms to prevent cyber-incidents

Introduction to ‘data’ and the cyber landscape

Regulation of data across the world


PIPEDA
State-specific legislation
GDPR
Federal Law No. 152-FZ on Personal Data
PRC Cybersecurity Law
Brazil’s General Data Protection Law Federal Law no. 13,709/2018 (LGPD)
Protection of Personal Information Act 2013 ("POPI")
Privacy Act
HEAVY
ROBUST
MODERATE
LIMITED
REGULATION & ENFORCEMENT

Introduction to ‘data’ and the cyber landscape

Regulation of data: a snapshot of the laws

Privacy Act 1988 (Cth)	Regulates the collection, handling and use of ‘Personal Information’
Spam Act 2003 (Cth)	Prohibits the sending of unsolicited commercial electronic messages (i.e. "spam") with an Australian link
My Health Records Act 2012 (Cth)	Healthcare providers accessing, processing and storing 'My Health Records' are subject to a mandatory data breach reporting regime
Various state and territory laws	For example Information *Privacy Act 2014* (ACT) and Privacy and Data Protection Act 2014 (Vic) that cover government

Introduction to ‘data’ and the cyber landscape

Regulation of data: *Privacy Act 1988* (Cth)

- Regulates the collection, handling and use of ‘Personal Information’
- Standards: 13 Australian Privacy Principles
- Regulator: Office of the Australian Information Commissioner (OAIC)
  www.oaic.gov.au (useful resources)
- Small business exemptions, but no general exemption for not-for-profits
- Regulates the notifiable data breach scheme (NDBS)

Introduction to ‘data’ and the cyber landscape

Regulation of data: the Notifiable Data Breach Scheme (NDBS)

APPLICABLE TO WHO?

APP entities subject to *Privacy Act 1988* (Cth)

WHAT TO INVESTIGATE

Suspected Eligible Data Breaches

WHEN TO NOTIFY?

As soon as practicable

WHO / HOW TO NOTIFY?

OAIC and affected individuals - by ordinary means

PENALTIES

Up to AUD 2.1 million civil penalty (organisations)

Introduction to ‘data’ and the cyber landscape

Regulation of data: the Notifiable Data Breach Scheme (NDBS)

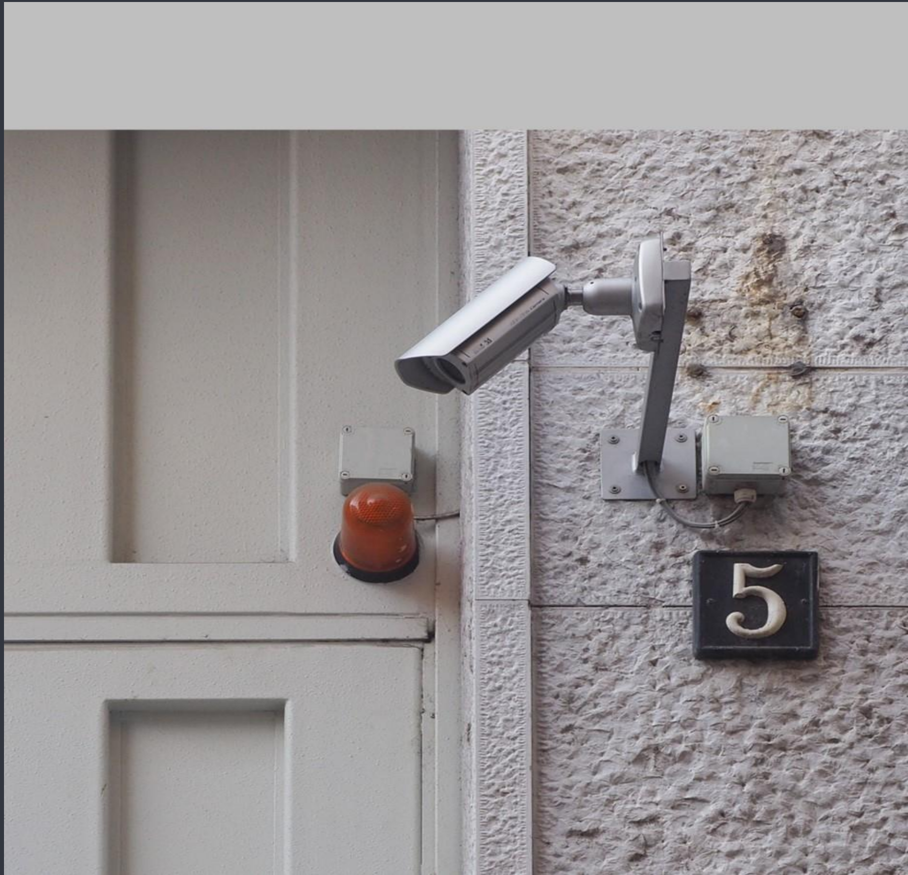
In order to assess whether there has been a notifiable breach, organisations must ask:

1. Has there been a data breach?
2. Is serious harm likely?
3. Can remedial action be taken to prevent likely risk of serious harm?

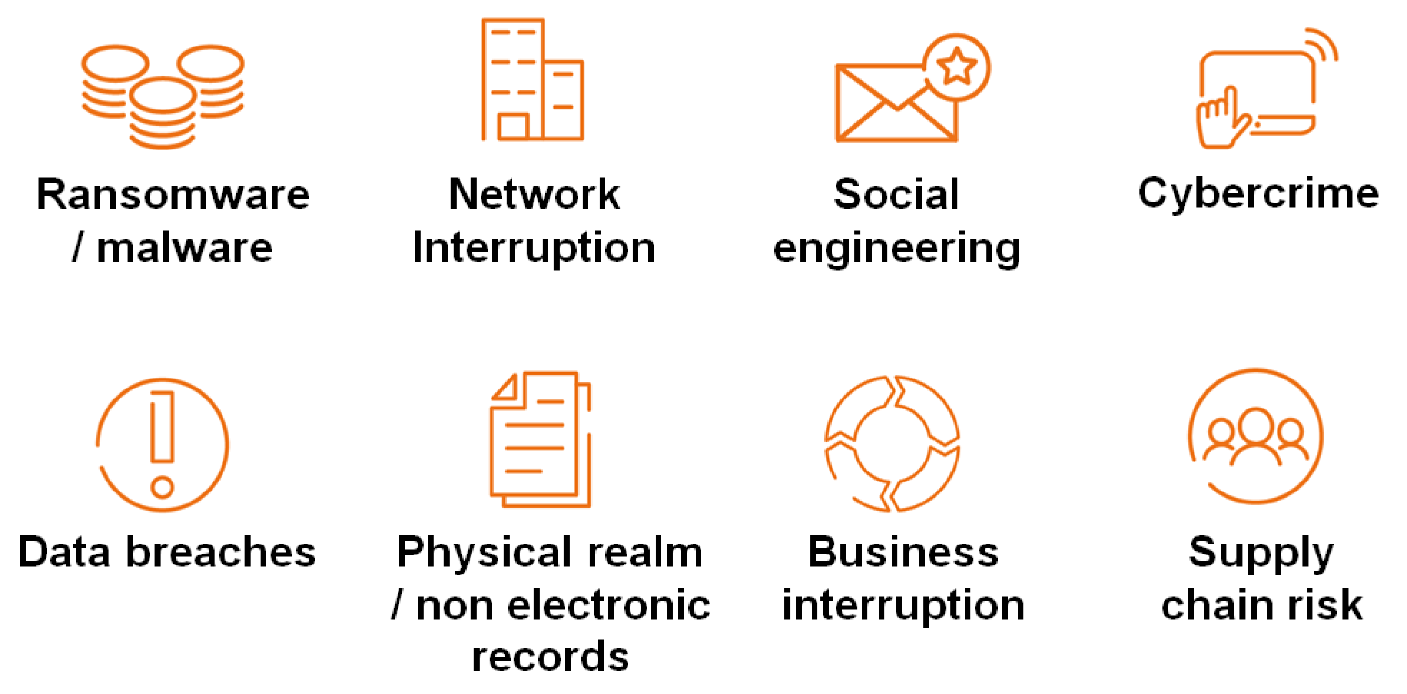
Introduction to ‘data’ and the cyber landscape

Proposed changes to the Privacy Act

- Increased penalties for all entities covered by the Act, which includes social media and online platforms operating in Australia
- Provide the OAIC with new infringement notice powers backed by new penalties
- Expand other options available to the OAIC
- Require social media and online platforms to stop using or disclosing an individual's personal information upon request
- Introduce specific rules to protect the personal information of children and other vulnerable groups
- These changes are being backed by an AUD 25 million increase to the OAIC’s funding over the next 3 years



Introduction to ‘data’ and the cyber landscape



Ransomware / malware

Network Interruption

Social engineering

Cybercrime

Data breaches

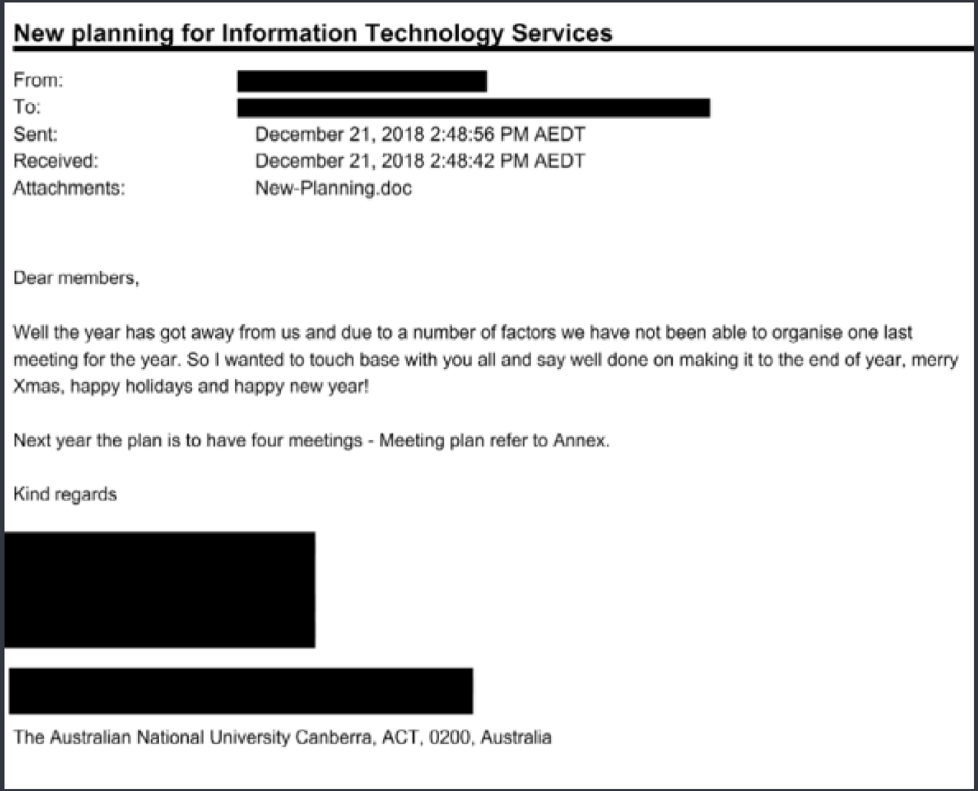
Physical realm / non electronic records

Business interruption

Supply chain risk

Introduction to ‘data’ and the cyber landscape

Example: Phishing email - ANU Data breach



New planning for Information Technology Services

From: [redacted]
To: [redacted]
Sent: December 21, 2018 2:48:56 PM AEDT
Received: December 21, 2018 2:48:42 PM AEDT
Attachments: New-Planning.doc

Dear members,

Well the year has got away from us and due to a number of factors we have not been able to organise one last meeting for the year. So I wanted to touch base with you all and say well done on making it to the end of year, merry Xmas, happy holidays and happy new year!

Next year the plan is to have four meetings - Meeting plan refer to Annex.

Kind regards

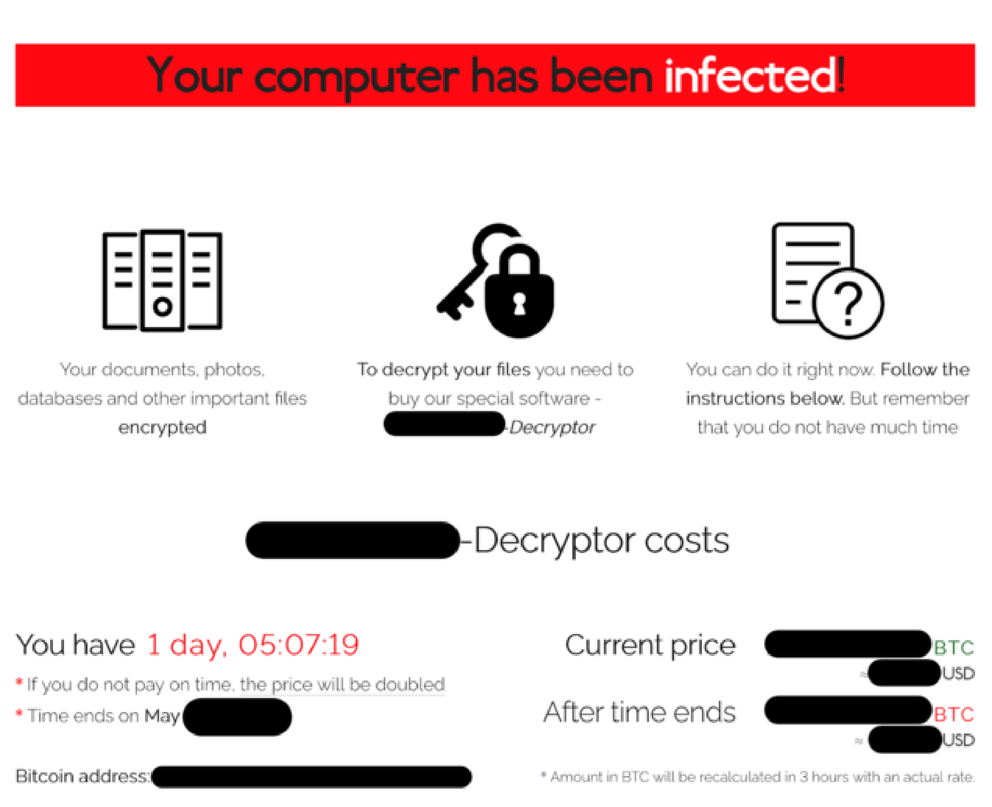
[redacted]

[redacted]

The Australian National University Canberra, ACT, 0200, Australia

Introduction to ‘data’ and the cyber landscape

Example: Ransomware



Your computer has been infected!

Your documents, photos, databases and other important files encrypted

To decrypt your files you need to buy our special software - [redacted]-*Decryptor*

You can do it right now. **Follow the instructions below.** But remember that you do not have much time

[redacted]-Decryptor costs

You have 1 day, 05:07:19

* If you do not pay on time, the price will be doubled

* Time ends on May [redacted]

Bitcoin address: [redacted]

Current price [redacted] BTC

≈ [redacted] USD

After time ends [redacted] BTC

≈ [redacted] USD

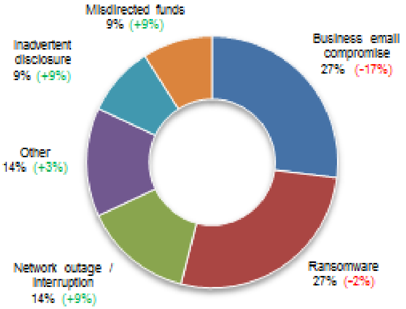
* Amount in BTC will be recalculated in 3 hours with an actual rate.

Cyber Monthly Update (August 2020)

CLYDE&CO

The Cyber Landscape - what we've been seeing this month*

Incident Types



Key Insights

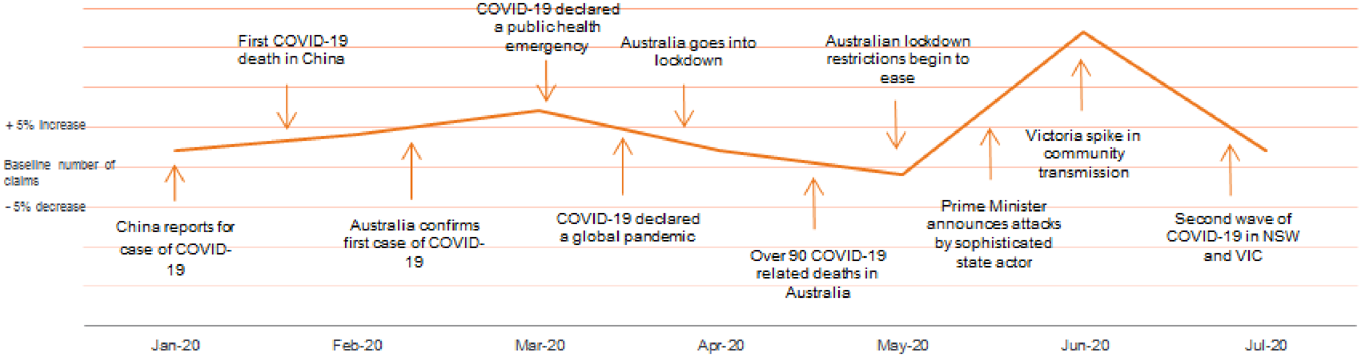
Greatest monthly increase in tech (+11%) and education (+9%) sectors.

- May be attributed to both sectors being of particular interest to foreign state actors.

Ransomware most common incident type alongside BEC.

- Number of ransomware incidents per month has doubled since January.
- This reflects OAIC NDB report - from January to June 2020, the number of notifications attributed to ransomware attacks increased by more than 150%.

Impact of COVID-19 on Number of Cyber Claims



First COVID-19 death in China

COVID-19 declared a public health emergency

Australia goes into lockdown

Australian lockdown restrictions begin to ease

Victoria spike in community transmission

China reports for case of COVID-19

Australia confirms first case of COVID-19

COVID-19 declared a global pandemic

Over 90 COVID-19 related deaths in Australia

Prime Minister announces attacks by sophisticated state actor

Second wave of COVID-19 in NSW and VIC

Key Updates

OAIC Notifiable Data Breach Report

Key takeaways

- Entities lacking understanding of IT systems, APPs and data held.
- Failure to comply with requirements of notification statements. Mitigation advice missing.
- Ransomware attacks morphing into data exfiltration. Assessment timing key.
- The OAIC is not aware of any evidence to suggest number of notifications has been influenced by COVID-19.

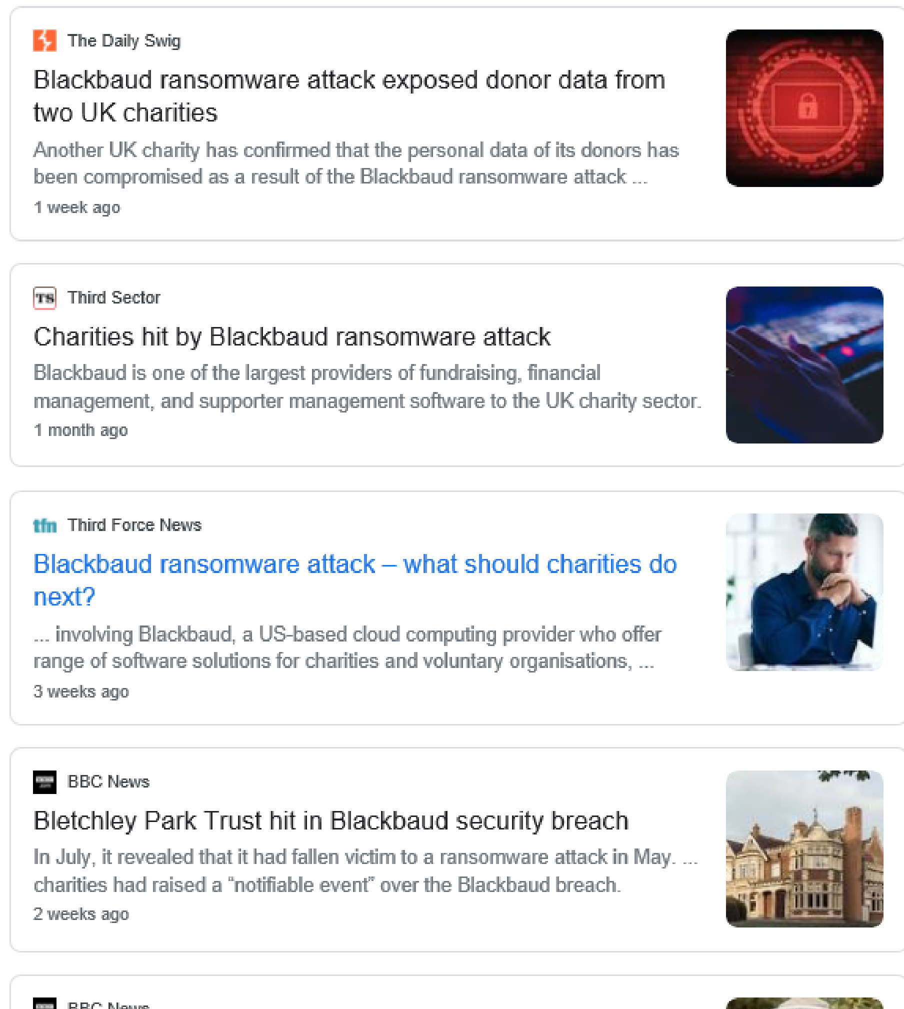
Australia's Cyber Security Strategy 2020

- Investment of $1.67 bn over 10 years in cyber security.
- Insurance industry overlooked but key.

**Data is based on new incidents we received between 1 – 31 July 2020.*

Introduction to ‘data’ and the cyber landscape

Case study: Blackbaud



The Daily Swig

Blackbaud ransomware attack exposed donor data from two UK charities

Another UK charity has confirmed that the personal data of its donors has been compromised as a result of the Blackbaud ransomware attack ...

1 week ago

Third Sector

Charities hit by Blackbaud ransomware attack

Blackbaud is one of the largest providers of fundraising, financial management, and supporter management software to the UK charity sector.

1 month ago

Third Force News

Blackbaud ransomware attack – what should charities do next?

... involving Blackbaud, a US-based cloud computing provider who offer range of software solutions for charities and voluntary organisations, ...

3 weeks ago

BBC News

Bletchley Park Trust hit in Blackbaud security breach

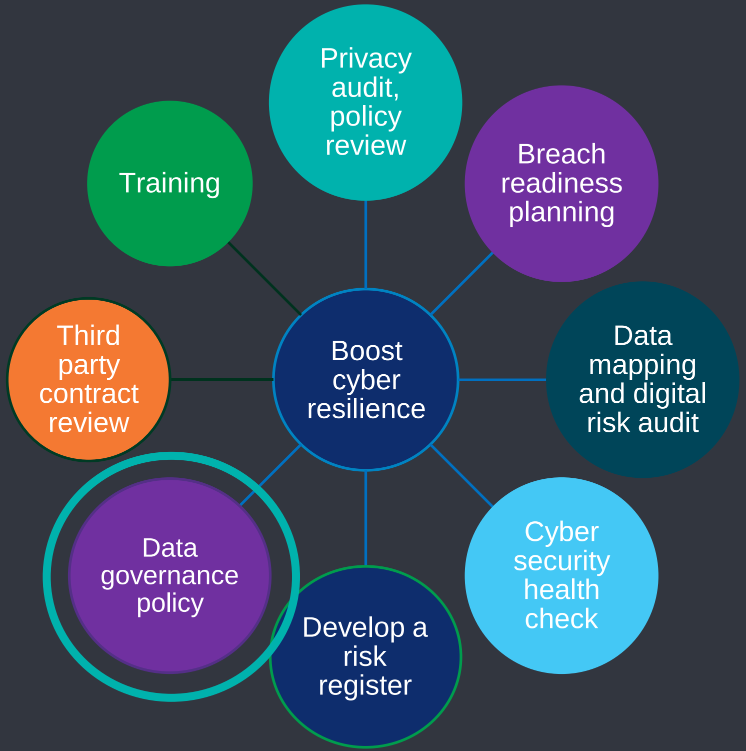
In July, it revealed that it had fallen victim to a ransomware attack in May. ... charities had raised a “notifiable event” over the Blackbaud breach.

2 weeks ago

BBC News

Introduction to ‘data’ and the cyber landscape

What can organisations do to prepare?



Boost cyber resilience

Privacy audit, policy review

Breach readiness planning

Data mapping and digital risk audit

Cyber security health check

Develop a risk register

Data governance policy

Third party contract review

Training

Data Governance

Community Legal Centres Queensland

Data Governance

What is ‘Data Governance’?

- Data Governance is the organisation and implementation of policies, procedures and standards for the effective use and protection of information.
- It is the process of organisation of an enterprise’s data, involving an enterprise-wide system of policies, procedures and controls to ensure that data is properly monitored, stored and managed.
- Governance should follow, reflect and cover the full life cycle of data.

Data Governance

Data Governance is different from ‘privacy law’ and ‘cyber risk’

- Data governance: processes necessary for effective information management across the whole company, for all types of data.
- Privacy: laws governing the appropriate use of personal information to protect individuals.
- Cyber risk: the risk of loss (such as financial, disruption or damage to the reputation of an organisation) from a failure of an organisation’s information technology systems.

Data Governance

Why is Data Governance important?

- Supports better decision-making and improves operational efficiency through data.
- Protects the needs of data stakeholders, in particular concerning privacy, confidentiality and access.
- Ensures the organisation adopts common standards and approaches to data issues.
- Ensures clarity and transparency with respect to access and usage of data.

Data Governance

Why is Data Governance important?

- Data is an asset and can be leveraged for organisational growth.
- The security of data is important – legal, regulatory and other implications if things go wrong.
- Consequently, data governance is starting to appear on the risk registers of companies across different industries.

Data Governance

Proper data governance allows organisations to take full advantage of the opportunities data provides and avoid the risks that come with data collection

Data Governance

Data Governance protects against a range of risks

- Missed opportunities
  - Loss of ‘competitive advantage’
  - Reduced efficiency
- Reputational risk
  - Loss of trust with donors, beneficiaries
  - Can change the perception of organisation as a safe source of donation/contribution to an risky one
- Legal and regulatory risks

Data Governance

Case study:
NSW Ambulance Service

- NSW Ambulance Service allowed a contractor widespread access to its records and databases.
- Sensitive personal and health information of NSW Ambulance workers was compromised, contractor was able to gather and sell the personal and health information of NSW Ambulance employees.
- Result: large class action settlement for employees, reputational damage to NSW Ambulance.

Data Governance

Data Governance provides a range of opportunities

Monetisation of data	Targeted ads; sale of data to analysts
Improved stakeholder loyalty	Personalisation, predictive suggestions (such as for donations or causes)
Internal provision of analysis	Fraud detection
Improved reputation	Perception as safe place to donate, and safe holder of personal information
Increase general efficiency	Proper data governance can allow entities to streamline operations

A framework for strong Data Governance

Community Legal Centres Queensland

A framework for strong Data Governance

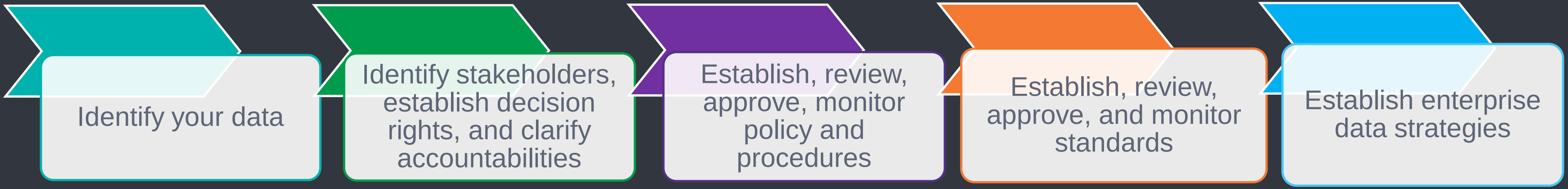
Data Governance will vary from organisation to organisation

It will depend on the data held and management priority:

- Data quality
- Privacy, compliance and security
- Data and business intelligence

A framework for strong Data Governance

Key components of a Data Governance framework



Identify your data

Identify stakeholders, establish decision rights, and clarify accountabilities

Establish, review, approve, monitor policy and procedures

Establish, review, approve, and monitor standards

Establish enterprise data strategies

A framework for strong Data Governance

Identify your data: example of data classification

SENSITIVITY LEVEL	DESCRIPTION
Public	Data which could readily be obtained from a public source such as a web site or directory.
Confidential	Data which has been gathered for business/operational purposes and would not normally be disclosed to third parties. This can be a sensible default for organisations and this level of protection is required unless specified otherwise.
Sensitive	Data which would cause harm if compromised: harm to the organisation, third parties, or both. Active measures are required for protection.
Protected	Data which would cause severe harm if compromised, such as widespread reputational damage or large financial loss. Access must be fully controlled and all disclosures tracked.

A framework for strong Data Governance

Identify stakeholders: types of Data Governance roles within an organisation

- Data Governance Council/Data Governance Board: to oversee data governance. This role is occupied by members of the board/committee of management or other senior staff.
- Data Manager/Data Owner: to control the data for the organisation, and to ensure data protection and integrity. This role is occupied by an officer of the organisation.
- Data Steward: to contribute business expertise and maximise the value of data to the organisation. This role is usually occupied by a person in senior leadership.
- Data Custodian: to protect and secure the data. This role is usually occupied by an individual with technical skills.
- Data User: to make use of data for business operations and decision making. This role may be any employee/worker.

A framework for strong Data Governance

Developing a Data Governance framework

- Clearly establish the goals and purpose: the overall vision and goals must be simple, clear and precise
- Only put governance where needed: select sponsors, owners and participants and establish processes focused on results; prioritise based on organisational need; do not apply governance solely to build consensus or to react to momentary interest
- Keep it simple and pragmatic: keep the governance model as simple as possible and make sure that all tasks are adding value to the overall organisation
- Design from top down but implement from the bottom up: design policies, standard and processes for the entire organisation; build and implement then practically starting with high impact areas
- Be flexible: recognise that a “one size does not fit all” when it comes to governance
- Provide clear communication: communicate the activities of the framework often to all relevant stakeholders

A framework for strong Data Governance

Developing a Data Governance framework

Ensure that you have a Data Governance Policy that applies to all employees.

This document should:

- provide rules and guidelines for ‘best practice’ for managing and collecting data;
- set out the procedures to be followed if there is suspicion of a data breach; and
- assign ownership of data, so that decision making authority is clear

Conclusion

Top tips

Understand that Data Governance is broader than ‘privacy’ or ‘cyber-risk’

Think about Data Governance as an opportunity for your organisation

If in doubt seek legal assistance

Questions?

Community Legal Centres Queensland