BreastScreen Victoria

Data breach and cyber disruption – preparing for the inevitable

Georgina Marr, CIO

BSA conference
March 2024

What do we mean?

Cyber security

Measures used to protect the confidentiality, integrity and availability of systems and data

System

A related set of hardware and software used for the processing, storage or communication of information and the governance framework in which it operates.

Australian Cyber Security Centre (ACSC)

Source - https://www.cyber.gov.au/learn-basics/view-resources/glossary Accessed 14 Mar 2024

Why?

- Reputation – trust
- Service continuity – Business disruption
- Information security - Data breach
- Compliance
- Funding

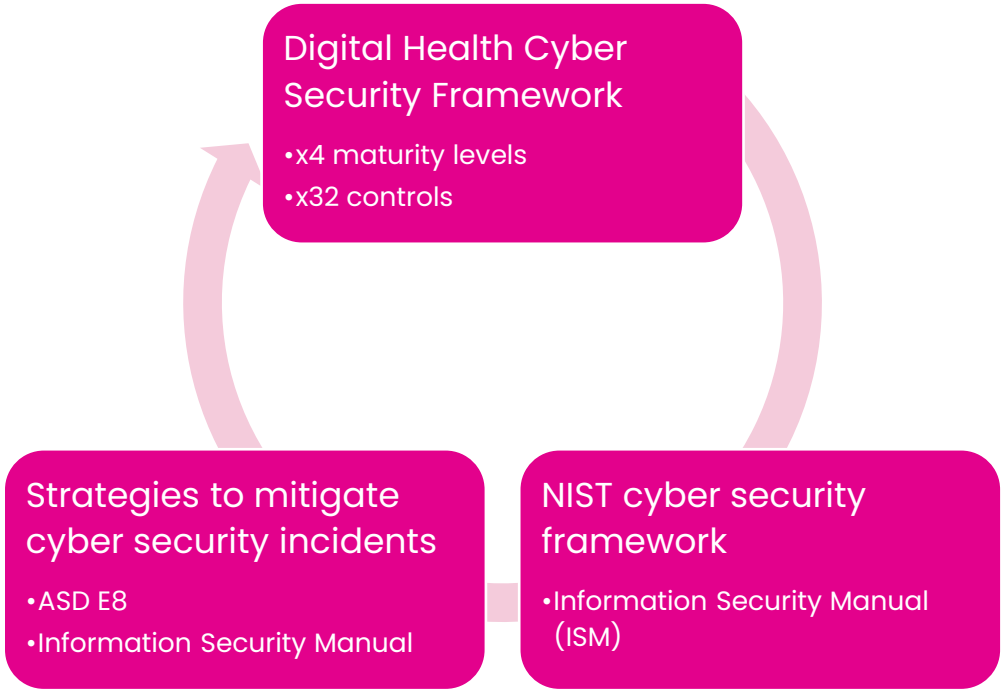
How did BSV approach?

Continuous quality improvement

1. Framework selection & adoption
2. Program overview - inception to operationalisation
    - Cyber simulation exercises
    - Data at rest self-assessment
    - Vendor security assessment
3. Access to expertise

Framework

Best practice - evidence informed



BreastScreen Victoria

Program overview

2017-18

- BSV Strategic priority
- Framework selection
- Independent review framework self-assessment & practice

2019-20

- Cyber security improvement project approved to uplift technology and capability; and provide assurance
- Joined Digital Health Cyber Security Program incl Annual self assessment

2021-23

- Audit self-assessment
- Annual self-assessment submission > 'live'
- Project > Program

Cyber security simulation exercises

Develop confidence – face fear

What

- Practice response to a cyber security incident – evolving process

Who

Decision makers (or delegates)

- Client engagement
- Clinical
- Communications
- Financial
- Governance & risk
- IT

When

- As often as you can afford

How

- Engage a third party – big four versus specialist
- 1-2 people to plan detail -realistic
- All in a room

Cyber security simulation exercises

Why?

- Practice
- Evaluation
    - People
    - Process
    - Systems (technology)
- Actions

Data at rest

Develop confidence – know where your data is stored

What

- Information that resides on media or a system – saved file, extract, system generated

When

- Establish a baseline and review periodically, consider audit

How

- Desktop exercise - DIY v engage a third party
- List all your software
- Approach your subject matter experts
- Approach your vendors
- Document the information stored – data elements, data collection period (start/end), classify the type and sensitivity of the data stored
- Assess risk – people, process, technology
- Consider a product owner

Data at rest

Why?

- Know where your data is stored
- Assess risk
- Training - gaps
- Ways of working

Vendor security

Develop confidence – understand your vendors approach

What

- Vet your vendors

When

- Every new software or hardware purchase (including services)

How

- Choose a framework
- Desktop exercise - DIY v engage a third party
- Document information flow and stored
- Assess risk – people, process, technology
- Consider a product owner

Why

- Know where your data is stored
- Assess risk – does the benefit of engaging this vendor exceed the risks? Are there sufficient controls in place – people, process, technology, compliance

Access guidance & expertise

- Australian Signals Directorate
  Australian Cyber Security Centre
- National Institute of Standards and Technology – Cyber Security
- ISO standard - Information security, cybersecurity and privacy protection (ISO/IEC 27001:2022)
- Department of Health
- Big four / Specialists
- CISO or vCISO

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

NIST National Institute of Standards and Technology
U.S. Department of Commerce

BreastScreen Victoria

Conclusion

- Conduct a cyber simulation exercise
- Build an inventory of where your data is being stored (and ideally how it moves around)
- Understand what data your vendors are storing and their approach to information security