protiviti®
Global Business Consulting

ASIC's cyber security survey: Key takeaways and quick wins

The results from the recent ASIC cyber security survey, '*REP 776 Spotlight on cyber: Findings and insights from the cyber pulse survey 2023*,' released on 13 November 2023, have once again highlighted the security posture of corporate Australia's management of cyber security. While there were some encouraging trends in specific security capabilities around identity and access management, governance and risk management and asset management, we will focus on some quick wins and remedial actions on the larger gaps that were prominent in the findings.

4 areas for organisations to focus on

1. Third-party risk management

The management of risks associated with third-party suppliers has always been a challenge for several organisations. Even some of the most mature organisations struggle to gain assurance on controls operated and managed by suppliers. Specifically, organisations do not comprehensively understand the ownership of controls. Organisations often rely on contractual provisions to transfer the risk when in fact the risk is owned and needs to be managed by the organisation. Questions around areas such as access to information, data residency, management of changes, control over data breaches are critical in assessing the risks associated with third-party suppliers.

Quick win strategies to build third-party risk management

- Develop a third-party risk management framework to articulate approaches for the following:
    - Building an inventory of suppliers for documenting and tracking relevant information.
    - Risk profiling of suppliers based on criteria including the criticality of services, access to information, and management of data.
    - Identifying controls to secure access to data, processes for data retention and disposal, end of contract requirements to remove or transfer data.
    - Designing metrics for monitoring and evaluating supplier performance and compliance.
- Establish a process to conduct risk assessments and obtain assurance through supplier security questionnaires, SOC2 reports, and independent audits.
- Document results from assessments to trigger confirmation and follow-up on exceptions.
- Design an approach to continuously monitor supplier services, commitments and changes to processes that might impact information security.

2. Data protection

Regardless of the size and nature of the business, organisations have had huge challenges in understanding data in their environment. Key questions on what data is held, where it's held, how long it's held and most importantly why it's held are left unanswered before protection mechanisms can be put in place. Some of the recent data breaches in Australia have provided the impetus for data management and the upcoming changes to Australia's privacy legislation will renew the focus.

Initial steps to enhance data protection

- Embark on a data discovery exercise to understand what data is held within the environment and develop a catalogue.
- Understand the processes that collect data and the business rationale to keep the data.
- Build an inventory of data across all critical and non-critical systems and map the data flow inside and outside the organisation.
- Identify controls to manage and protect data such as encryption at rest and in transit, anonymisation, isolation of backup, longevity of logs, and location of data.
- Determine the need to design and implement additional controls to classify and mask data and prevent data leaks.

3. Incident response

The biggest challenge in incident management is the lack of preparedness to both detect and respond to an incident. While organisations focus on building a response plan, the emphasis should be on the ability to detect events that may translate into incidents. A greater analysis of events and alerts would enable organisations to study the patterns and predict occurrences proactively to help them respond to incidents effectively. As an example, if traffic patterns in and out of the network are analysed in detail, attempts to infiltrate can be detected and thwarted early on.

Ingredients for a strong incident response plan:

- Define roles and responsibilities, incident types, incident categorisation/ prioritisation.
- Establish an incident response team with protocols for escalation.
- Evaluate 'what-could-go-wrong' scenarios for all critical changes, and check if there is a response to each question.
- Implement solutions for incident detection and reporting mechanisms.
- Design the process for triaging, containing, recovering and eradicating the incident.
- Determine root cause, document and socialise lessons learned.
- Conduct regular testing and validate the effectiveness of the plan.
- Develop playbooks for specific scenarios such as ransomware, or critical infrastructure outages.

4. Framework or standard adoption:

There has been renewed focus among organisations regarding assessing security posture against leading standards, and adopting a framework that will help drive strategies towards enhancing their position. The biggest challenge is in identifying the most relevant standard or framework that will provide optimal benefits to both internal and external stakeholders.

Where to begin

- Assess regulatory obligations and customer requirements as this will drive focus on appropriate standard to comply with.
- Determine the criticality of service delivery - what do your customers care about?

- If it's still unclear, start with the ISO 27001 standard or Essential 8 to gain an understanding of baseline controls that can be designed and implemented for establishing an information security management system.

Closing thoughts

ASIC's survey is yet another eye-opener on why information security is of paramount importance given some of the recent data breaches, malware attacks and privacy concerns. The implications of these incidents are widespread and steps should be taken in earnest to enhance security posture and avoid pitfalls. The brief recommendations made above are starting points in addressing the concerns from the survey and can be supplemented with a more robust design and implementation of controls. Taking these steps will help organisations make a beginning in their journey towards information security and create a secure environment for everyone.

Contacts

Krishnan Venkatraman
+61 450 204 911
krishnan.venkatraman@protiviti.com.au

Shane Silva
+61 402 496 669
shane.silva@protiviti.com.au