Cyber Security Controls

The role of policy, collaboration and engagement in cyber security

Leonie Shepherd
Technology
Objective Insight
Australia
anne.objectiveinsight@gmail.com

Abstract— **In Australia, Cyber-attacks are increasing with devastating impact to some business. The Australian Signals Directorate's Australian Cyber Security Centre (ACSC) [4] is running a survey to understand what small to medium sized businesses want or need to tackle cybercrime. They report that "the level of knowledge about good cyber security practices remains fairly low with the majority of businesses believing they are safe from cybercrime because they use antivirus software". These companies would employ people who can assist in minimizing cyber-attacks when they are engaged via effective policies and frameworks with a focus on engagement between the owners and users of the policies to ensure they are fit for purpose, easy to understand and follow. The ACSC also drives cyber security awareness. However enhanced collaboration across organizations and industry to combine skills and knowledge would further assist in effective cyber resilience with metrics help to focus people on the desired outcomes.**

Keywords-APRA; CPS234; policy; engagement.

I. INTRODUCTION

Every person that accesses the systems and data in organizations represent some kind of cyber security risk. Organizations rely on their people to identify potential cyber risks and take the appropriate steps aligned to their requirements. Therefore business and technology processes need to be regularly reviewed to identify where things can go wrong with a focus on the user of the policy and framework via workshops and awareness programs for example.

The use of entity level controls will assist in minimizing cyber risks. The nature of controls can be either preventative or detective and act as management's primary line of defense. This includes effective frameworks, policies and procedures that are fit for purpose and the reality of the situations they are meant to cover with options for contributions to assist in improving their effectiveness as a part of changing organizational culture to be more cyber resilient.

A control is an action taken by management to mitigate an inherent risk and/or satisfy an obligation. A control either reduces the likelihood of the risk occurring or reduces the potential impact if the risk occurs. It needs to be proportionate to the risks faced and designed to support strategic objectives. The ACSC survey highlights potential gaps and weaknesses in current processes and capabilities that result in cyber-attacks. This is one of a number of initiatives by the Australia Government. The Australian Prudential Regulatory Authority (APRA), who has a remit by the Australian government to regulate consumer banks, business banks, insurance companies, hedge funds, investment banks and superannuation providers, introduced Standard CPS234 for all APRA regulated entities effective 1 July 2019. The key obligation under CPS234 is that regulated entities must maintain information security in a manner commensurate with the size and extent of threats to its information assets, and which enables the continued sound operation of the entity. It applies to all information assets regardless of whether they are material business activities or not and assets managed by third parties [1]. APRA regulated businesses also rely on their people to know and do the right thing to protect companies from cyber-attacks. The Office of the Australian Information Commissioner (OAIC) [2] report that only 5% of data breaches notified under the NDB scheme from 1 April 2018 to 31 March 2019 were due to system faults however 35% were due to human error.

The rest of the paper is structured as follows; Section II introduces the need to focus on the people that organizations rely on to be more cyber resilient and the requirements of APRA regulated entities as cyber-attacks have increased on financial organizations Section III presents a proposal to more effectively collaborate and engage across and within organizations to help them to be more cyber resilient. Section IV concludes the paper.

II. COLLABORATE AND ENGAGE

Effective engagement between policy owners and the people required to understand and follow the policy will assist in minimizing potential cyber risks. This includes creating a culture where people can and will work together to share specialized knowledge and experience just as the cyber criminals work together. Furthermore, it is increasingly important for organizations to collaborate with each other and with their people to gain new insights and connections to better protect their systems and data as the cost of cyber-crime increases. This includes supporting effective governance of outsourced services and reviewing contracted arrangements aligned to policy and frameworks.

A. *APRA regulated organizations*

APRA regulated organizations, under CPS234, are required to ensure their policies, standards, guidelines and procedures pertaining to information security are in order and aligned to their exposure to threats. An effective policy

ISBN: 978-1-61208-743-6

framework is important to manage potential risks, as it includes responsibilities of stakeholders to whom the framework applies including Board, senior management, governing bodies and individuals. This would include categorizing and managing data classifications and supporting employees to understand and manage their data appropriately, particularly customer related or sensitive information. Therefore, policies need to be accessible, effective, streamlined, simplified so that they are easy to understand and follow, enforceable, written in plain English and tied to employee metrics (key performance indicators) to support behavior changes.

In an APRA regulated entity, Boards are ultimately responsible for information security. However, they rely on their employees and sometimes on a third party provider to understand and adhere to their organizational policies and procedures. They rely on frameworks being reviewed and tested by the framework owner on an annual or more frequent basis where required and effective governance. The use of outsourced service providers does not eliminate management's responsibility for maintaining effective controls over material inherent risks or compliance with laws and regulations [1].

B. Notifiable data breachess

Process level controls need to be in place to ensure or verify that appropriate actions have been taken when executing a process or to recover from errors or irregularities. For example, APRA says that the cyber security measures in CPS234 will help APRA-regulated entities to repel cyber adversaries, as well as handle incident response swiftly and effectively if a breach occurs [1]. This follows an increased number of cyber-attacks. Since Australia's Notifiable Data Breaches (NDB) scheme launched in February 2018, the Office of the Australian Information Commissioner (OAIC) advise that 964 data breaches were reported between 1 Apr 2018 and 31 March 2019, which is a 712% increase in reported data breaches. The main sources of the data breaches were attributed to malicious or criminal attacks (60%), phishing and spear phishing (153), credentials obtained by unknown means (28%) and human error (35%). OAIC report that 83% of data breaches affected fewer than 1,000 people. However, 86% of notifications involved disclosure of contact information. The finance sector accounted for 41% of data breaches compared to a 35% average for all sectors. OAIC advise "The predominance of human factors in data breaches emphasizes the importance of education and training for all employees who handle personal information." [2]

The goal of CPS234 is continued information security management and improvement, investment aligned to the sophistication of the cyber-attacks and risk management. APRA expects these entities to ensure the security of all customer data". APRA must be notified as soon as possible but no later than 72 hours after becoming aware of an information security incident that did or had the potential to materially affect a stakeholder [1]. OAIC report that "most data breaches—including those resulting from a cyber incident—involved a human element, such as an employee sending information to the wrong person or clicking on a link that resulted in the compromise of user credentials". [2].

III. PROPOSAL

Considering how long cyber security has been highlighted, yet more organizations are victims of cyber-attacks, perhaps there is an opportunity to more effectively collaborate and engage across organizations and within organizations with a focus on the people they rely on to assist them to be cyber resilient, for example via awareness. This may include guidance on how organizations, which hold customer or sensitive data, could run a diagnostic gap analysis against their current cyber security governance framework. For example, running an assessment to identify potential gaps and weaknesses in current processes and capabilities related to:

1. Reviewing roles and responsibilities such as actionable roles and escalation processes
2. Information security capability such as how internal and third party risk assessments are conducted. How vendors are tiered according to risk
3. Policy framework such as the location of the organisational frameworks covering vulnerabilities and threats – how is this stored and maintained, who has access to it in what format. This includes the owner details correctly and clearly recorded for queries and feedback
4. Implementation of controls such as how vulnerabilities and threats are detected then classified and measured.
5. Review and update information security policies, procedures and controls for example including one or a combination of the following:

a. Walk through processes from start to finish with the people performing the activities to collect evidence of how activities that minimise cyber security risks are performed. This provides assurance that all controls and potential control gaps are identified. Once controls are identified and documented, link them to the relevant risk. This includes ensuring adequate cyber security mechanisms where a supplier manages data or systems

b. Ask questions aimed at getting relevant information from the people performing the activities in order to identify the points in the process where things can go wrong and the actions that have been designed to prevent, detect and recover from these errors.

c. Review existing policies, procedures, standards and guidelines for adequacy of information security controls such as via conducting workshops to discuss changes to the business environment, risk, controls and any potential issues

6. Review contracts with service providers. Test their security controls and evaluate their governance processes if they manage organizational assets.

7. Run awareness campaigns aimed at ensuring policies and frameworks make sense, clearly set out what is required, support delivery of what is necessary and clarify where and how to make a positive contribution to improve it. Combine this with metrics supporting behavior changes. Ongoing monitoring would provide feedback on the effectiveness of the campaigns..

IV. CONCLUSION

Using APRA CPS234 guidelines or similar, organizational testing of information security capability and policy framework in terms of people, processes and technology at the most fundamental level is important to combine the various initiatives. Clearly defined, documented policies, standards and procedures with the end-user in mind support management requirements (information threats, technical and procedural vulnerabilities). Aim for a balance of benefit versus risk of each control when reviewing results as a part of ensuring confidentiality, integrity (accuracy and freedom from unauthorized change or usage) and availability (access and usability when required).

REFERENCES

[1] Australia Prudential Regulation Authority (APRA), “Prudential Standard CPS 234 - Information Security (Draft)”, 2018, Available from: https://www.apra.gov.au /sites/default/files/Draft-CPS-234.pdf

[2] Office of the Australian Information Commissioner (OAIC) “Notifiable Data Breaches scheme 12-month insights report”, Available from: https:///www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-scheme-12month-insights-report//

[3] Smart Collaboration: Breaking Down Silos - Heidi K. Gardner

[4] The Australian Signals Directorate’s Australian Cyber Security Centre (ACSC), available via https://www.cyber.gov.au/