Submission
No 23

INQUIRY INTO CYBERSECURITY

Organisation: ISG Consulting Pty Limited

Date Received: 20 September 2020

Ms Charlotte Wood
Director, Policy and Awareness
Cyber Security NSW - Service NSW
GPO Box 7057
Sydney NSW 2001

Introduction

As the first company admitted to the NSW Government Information Security Panel in 2002, we have implemented policy (and in many cases interpreted high level guidance) using a risk-based model in accordance with AS4444 / AS7799 and later ISO27001. We were also one of the advisors on the remodeling of the ASCI33 Commonwealth Security Guidelines into the current Information Security Manual. During this period, we have advised NSW Police, NSW Ombudsman, ODPP, NSW Education, Sydney Water, Transport for NSW, and NSW Health. In 2013 we were selected in a selective tender process to manage the integration of the separate IT functions of agencies now making up Transport for NSW, and have subsequently advised on the integration of the security policies across the new Transport for NSW agency. We are currently engaged as cyber security advisors to TransGrid NSW for their IT and OT Security.

Given the emergence of new Cyber Security threats within the Australian business and government landscape, we would strongly urge the NSW Government to address the development or adoption of Governance models which address threats within an integrated governance model that can be implemented across the entire enterprise.

We commenced developing in 2013 a comprehensive suite of standards, processes, and work items for implementing Information Security, based around ISO27001, ITIL, and COBIT. These were developed with one of the NSW Transport entities and are available to assist other agencies to streamline implementation of these standards. These reference open standards such as OWASP, COBIT, ITIL, and ISO27001. A high-level framework has been published to the public domain through ISACA to facilitate its adoption.

Finally, we work with NSW Government technology partners Micro Focus and Microsoft who have technologies that can leverage and assist with implementation of these frameworks.

We are happy to provide further information and assistance around these ideas and strategies.

John Frisken

Director - Professional Services
Information Systems Group

Milton Baar

Director - Professional Services
Information Systems Group

Overview

Currently we perceive the main issue facing the NSW Government in cyber security is one of fragmentation. While many commentators high light the number of separate bodies responsible for tracking and managing cyber security as the main issue, we perceive an even greater issue of fragmentation relates to "technology domain", that is IT vs OT vs IOT. The term Cyber Security was originally coined to embrace all these domains, rather than Information Technology.

The NSW Cyber Security Standards do reference the need to implement an "Information Security Management System" (ISMS) or "Cyber Security Framework (CSF)", with scope at least covering systems identified as an agency's "crown jewels".

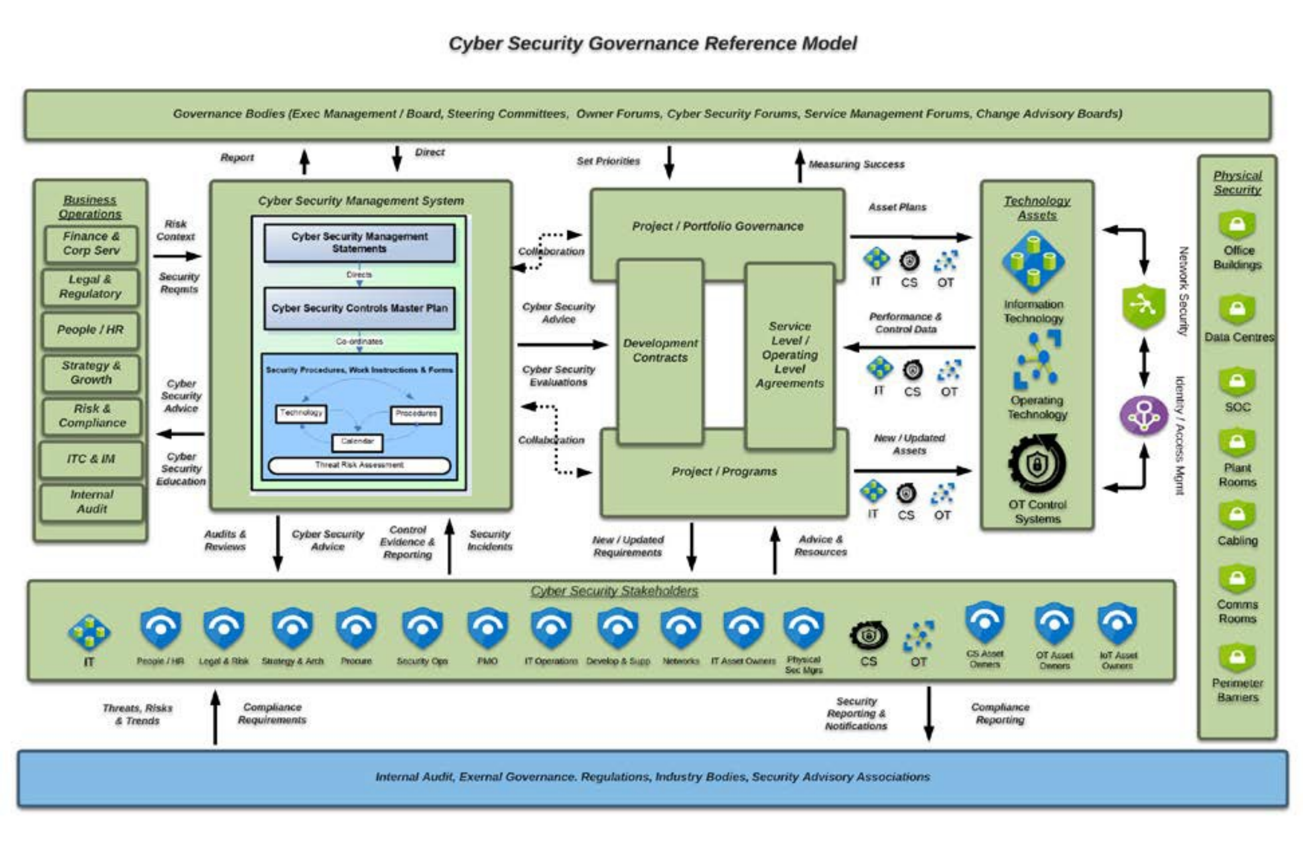
Our concern is that fundamentally these areas remain separate within most organisations. Twenty years ago, these areas were in fact only loosely coupled, if in fact they were coupled at all. In this environment there are few downsides to managing them separately. However, in the recent past these areas have become much more integrated, driven by converging technology, common use of the Internet, and a drive for cost efficiencies which is understandably demanding that supervisory managers and systems should utilise a shared service model. The problem is that these areas still have separate standards that define how these risks are identified and technology governed. Yet within large enterprises the forces mentioned above are driving these areas together without any commonly agreed approaches as to how they can be managed.

In 2015 ISG published into the public domain the results of over a decade of work in Cyber Security, much of it conducted in the NSW Government. One of the key concepts we developed was a multi standard approach to managing controls using the concept of a Controls Masterplan. Our research can be found in ISACA, **https://www.isaca.org/resources/news-and-trends/newsletters/ cobit-focus/2015/leveraging-cobit-to-implement-information-security**. An outline of the recommended program structure is defined in this article, which is Part 3 of a 4-part set of articles. Shown on the next page is a model built on this work incorporating explicit control sets from ISO27001 as well as IEC 62443. These models have been implemented in several large utility-based business units within the NSW Government managing critical infrastructure. But still we find difficulty in driving cohesive governance structures within these organisations owing to discipline and political factors within those organisations.

ISG has worked with the Education Sector for many years. The security challenges in education are complex because the network boundaries are blurred through the use by students and teachers of BYOD devices. The protections built into the devices need to follow the students and teachers wherever they are connected, not just when they are connected to school networks.

This requires innovative technology and leveraging partners who have ubiquitous presence across the globe. We are finding that cloud security solutions, including components such as the Enterprise Bus, are increasingly required to be leveraged to connect the school systems that are often hosted solutions.

Business and government enterprises face similar challenges as their organisations increasingly adopt cloud computing as a way of re-engineering their processes to reduce costs, increase flexibility and respond more quickly to their changing customer requirements. Like education, BYOD is also becoming much more common, although large corporates still mostly provide employees their devices, except for their Smartphones. The increasing use of home-based work that COVID-19 has spawned will become an increasingly prevalent model as organisations strive to provide greater flexibility to their work forces and reduce the cost of CBD based accommodation. This too will present security challenges for many organisations as they find their enterprise models morph to include participants who are transiently connected through VPNs or other channels.



The traditional trust models for implementing security require components engineered to support virtual networks and terminals. Keeping technology updated with the latest patches for network security and client devices becomes exponentially more difficult in this environment. The possible threats scenarios are also multiplied as this virtual network of devices continues to evolve.

The ASD Essential 8 was introduced to provide a checklist for businesses and smaller government organisations to mitigate common vulnerabilities. One of the reasons why the ASD Essential 8 has been so slow to be adopted is because of the complexity today of even simple environments and that attacks have evolved since the publication of the ASD Top 4 . There are no published case studies to implement these controls across the many different types of platforms that users interact with specific to the ASD Essential 8.

What is required to drive outcomes in Cyber Security are not checklists but processes focused around driving accountability for ensuring resilience in cyber defences. In large government departments we still see major short comings in processes for technology procurement which do not place responsibility for vendors to comply with standards nor implement review processes internally to check compliance. In such an environment cyber resilience will never be achieved until basic accountabilities are recognised and processes put in place to monitor them.

Changes to Current Strategy

The inclusion of NIST in the current NSW Government Cyber Security Strategy could be improved. As one of the leading Cyber Security advisors to the NSW Government we are quite confused as to why this change was originally made. We acknowledge that NIST is widely supported in the US, however it is causing confusion by its inclusion in the NSW Government Cyber Security strategy which should be addressed. There are three major problems with the inclusion of NIST as the NSW Government Cyber Security Framework:

1. NIST is a North American standard whereas ISO 27001 and IEC 62443 are European. ISO standards have a Plan-Do-Check-Act set of phases throughout all standards, which permits common management systems to be developed across all standard areas. This leads to enormous cost and efficiency savings for large enterprise who are required to maintain systems for managing multiple standards. NIST has its own set of phases, which while logical, is not is sync with European standards, which Australian Governments and Private Sectors have traditionally supported. This imposes significant cost and efficiency burdens on large agencies for little or no benefit. In fact, it could be argued that its inclusion is a net negative benefit due to the confusion it causes.

2. NIST has not been developed within a Certifiable Framework, like ISO standards, and therefore there is no mechanism for legal enforcement by the NSW Government, which is a significant drawback of the standard compared to ISO27001. IEC 62443 likewise cannot be certified either, but is largely implemented in conjunction with ISO27001, which addresses this problem.

3. In implementation of IEC62443 in large NSW Government agencies like Transport for NSW, we have found that NIST as a standard is incompatible and was removed from policy objectives. It is very confusing and not at all satisfactory to have a set of standards mandated by the peak standards setting agency which in fact cannot be implemented practically.

It could be validly argued that NIST has some advantages of ISO27001 and to a lesser extent over IEC 62443, but in that case, we would recommend that the NIST control set was implemented rather than the NIST process. This would in effect remove most of the problems noted above. We would recommend that the multi-standard certification framework developed for the NSW Government by ISG and referenced above would be the most efficient and cost-effective way to achieve this.