Chapter 24
Practical Align Overview of the Main Frameworks Used by the Companies to Prevent Cyber Incidents

Rogério Yukio Iwashita
University of São Paulo, Brazil

Luiz Camolesi Junior
University of Campinas, Brazil

ABSTRACT

Among the biggest cybercrime or information security challenges, the information security professionals must be up to date with the new risks, cases, and different ways of attacks. Being up to date in this complex and aggressive scenario is a huge challenge and is a necessity to the security professional to fight against the cybercriminals. Additionally, based on this standard of requisites to start an information security program, an immature professional may be confused on the different frameworks used by the industries, mainly ISO/IEC 27000 family, NIST 800-53, NIST Cybersecurity Framework, COBIT, etc. This chapter will help the information security professional to decide where is important to focus efforts, to decide what is feasible and which control does not demand any additional investment. Additionally, this grade helps the InfoSec professionals to compare the information security maturity level within the companies and between the companies, comparing with benchmarks.

INTRODUCTION

Probably the most known standard used by most companies to improve the information or cyber Security program is the ISO/IEC 27000 family. This standard which is derived from a British standard of 1999 is commonly used due the international certification which provides to external entities, a holistic view of the company security level. Today, the ISO/IEC 27000 family is composed by more than 40 standards,

DOI: 10.4018/978-1-7998-5728-0.ch024

normalizing diverse topics, since the Information technology – Security Techniques – Information security management systems – Requirements (ISO/IEC 27001), Network security (ISO/IEC 27033), Incident investigation (ISO/IEC 27043), among other topics. Nowadays, the newest ISO/ IEC 27000 standard is the ISO/IEC 27701, which propose a set of controls to the Information Security management systems focusing on the data privacy, which may reply to the nowadays demand of data privacy requirements, mostly to respond to the new European laws (GDPR) and many other similar privacy policies around the world.

The National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce maintains the known publication NIST Special Publication 800-53 Revision 4 since 2013 (last revision was on 2015) which is a set of security controls, including the description of and a suggestion on how to measure, implement and administer these controls. Although this publication describes the how-to, it also helps to delimiter the customization of these controls, explaining in details the reasons, risks and key points to success on the main goal: protect the assets of the company, but most providing the reader the ability to improve or optimize it for their own purpose and goals.

More recently, in 2014, due a USA Executive Order, a Cybersecurity framework (CSF) were created consolidating the best practices of different industry sectors and government. As the consequence, this framework is aimed to the security focused on the business and also on the privacy of the people. The components of a Cybersecurity framework are the "Framework Implementation Tiers" topic which may provide a holist view of the implementation of each control, grading from 1 (Tier 1) to 4 (Tier 4).

This chapter will demonstrate that these standards, even with more than twenty years they still must be used, describing when these frameworks should be used, explaining and detailing each standard, and most focusing on the implementation, success cases where these standards helped to avoid (or mitigated substantially) real incidents; lessons learned, with cases based on the prior scenarios, using known cases and my vast experience as Information Security Manager and CISO of great companies.

BACKGROUND

The ISO/IEC 27000 is the most known and used framework of Information Security and Cybersecurity Managers. Being used as the most comprehensive and in-depth framework in different companies.

As this family of standards have more than 40 different standards, this chapter will focus only on the ISO/IEC 27001 which focus on the requirements and security techniques of the information security management systems on information technologies. Also, this is the unique standard eligible for the accredited certification, which is a very good manner to assess and to present to possible customers that the Information Security controls and cares are in place properly.

The NIST SP 800-53 is a set of controls focused on security and privacy and it defines its deliverable as "*catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyberattacks, natural disasters, structural failures, and human errors. The controls are customizable and implemented as part of an organization-wide process that manages information security and privacy risk. The controls address a diverse set of security and privacy requirements across the federal government and critical infrastructure, derived from legislation, Executive Orders, policies, directives, regulations, standards, and/or mission/business needs. The*