INVENTORY AND CLASSIFICATION OF CYBER SECURITY STANDARDS

Independent summary to the final report

Authors:
Dr. B. Hulsebosch, CISSP
A. van Velzen, M.Sc.

May 20th, 2015

Commissioned by:
The Ministry of Security and Justice of the Kingdom of the Netherlands
Scientific Research- and Documentation Centre
Project number 2552

THE IMPORTANCE OF STANDARDS FOR CYBER SECURITY

Dutch society has increasingly become dependent on information technology (IT) systems. This constitutes the cyber domain: the informational infrastructure of computer systems and telecommunications networks. Consequently, this dependency leaves society vulnerable to outage or malicious use of systems and has resulted in an increasing need for cyber security measures. Cyber security involves preventing damages from disruption, failure or abuse of IT, and recovery in case of eventual damages.

To make cyber security measures explicit, written norms are required. This allows implementation of measures in an optimal fashion and without having to resort to reinventing the wheel. These norms are cyber security standards: generic sets of prescriptions for an ideal execution of certain measures. Standards may take form as best practices, guidelines, methods, reference frameworks, etc.

Deploying cyber security measures according to standardized norms is deemed sensible. Standards ensure efficiency of security, facilitate integration and interoperability, enable meaningful comparison of measures, reduce complexity, and provide structure for new developments. Standardization also allows for safe and reliable cooperation in the cyber domain based on well-defined frameworks and agreements.

Over one thousand cyber security standards exist worldwide, begging how to see the forest for the trees. The present study thus seeks to provide an overview of cyber security standards. The question we ask ourselves is: which standards for cyber security are available nationally and internationally and how could these standards be positioned relative to each other? The approach taken comprised of several phases. Firstly, available cyber security standards have been tallied from 25 extant overview studies. Subsequently, a classification framework was developed according to which standards may be contrasted. The framework was thoroughly put to the test through interviews and expert sessions. Furthermore, the classification framework was operationalized into a step-by-step guide to select standards for implementation. Finally, the results were delivered as a report presented here in summary.

INVENTORY OF CYBER SECURITY STANDARDS

To gain insight into the most prevalent national and international standards for cyber security an inventory was composed based on 25 existing overview studies. From these a list of over 180 standards was drawn. An excerpt of the top ten standards most cited is given in the table below.

Title	Source	Origin	Language	Type	Vital Sector
ISO/IEC 27002	ISO/IEC	International	English	Standard	General
ISO/IEC 27001	ISO/IEC	International	English	Standard	General
NERC CIP 002 - 009	NERC	USA	English	Standard	Energy
NIST SP-800 series	NIST	USA	English	Guideline	General
ISA/IEC 62443	ISA	USA	English	Framework	Industry
AGA No. 12	AGA	USA	English	Best practices	Telecommunications
COBIT 5	ISACA	International	Multiple	Method	General
ISO/IEC 15408	ISO/IEC	International	English	Standard	General
API 1164	API	USA	English	Standard	Energy
PCI-DSS	PCI	International	Multiple	Standard	Finance

SEEING THE FOREST THROUGH THE TREES: THE CLASSIFICATION FRAMEWORK

From the large number of standards tallied it is gathered that the cyber security domain is complex and diverse. This makes it difficult to select standards or determine where standardisation is insufficient. The classification framework supports an overview of cyber security standards and allows to position them relative to each other.

Since such a classification framework could not be found until now, it was developed as part of this study. To this effect a number of relevant classifying dimensions have been identified. The first dimension concerns several variables that describe standards in an unambiguous manner. Think of variables such as origin, type, vital sector a standard pertains to or availability.

The second dimension regards the breadth of the standard in terms of intended goals for which the standard prescribes measures. These goals are prevention of incidents, taking measures, detecting undesirable activities, and responding to incidents. Several general standards cover this whole range of goals, such as ISO 27001 and COBIT. Using such a general standard a baseline for cyber security may be established. Moreover, several more specific focal areas can be determined for each goal. These are areas of activity where different specific cyber security measures are required. Examples are standards for risk assessment, identity and access management, or business continuity. No common classification exists for such focal areas; they are usually defined by the general standard(s) used to establish a cyber security baseline. The comparative relevance of different focal areas depends on the risk profile of the organization and may be different for each vital sector.

The third dimension stems from the organizational and operational embedding of cyber security standards and represents the depth (or specificity) of a standard. Here several layers could be distinguished: (strategic) governance; (tactical) management; (operational) people, processes and technology. Which results in the following model of the classification framework:

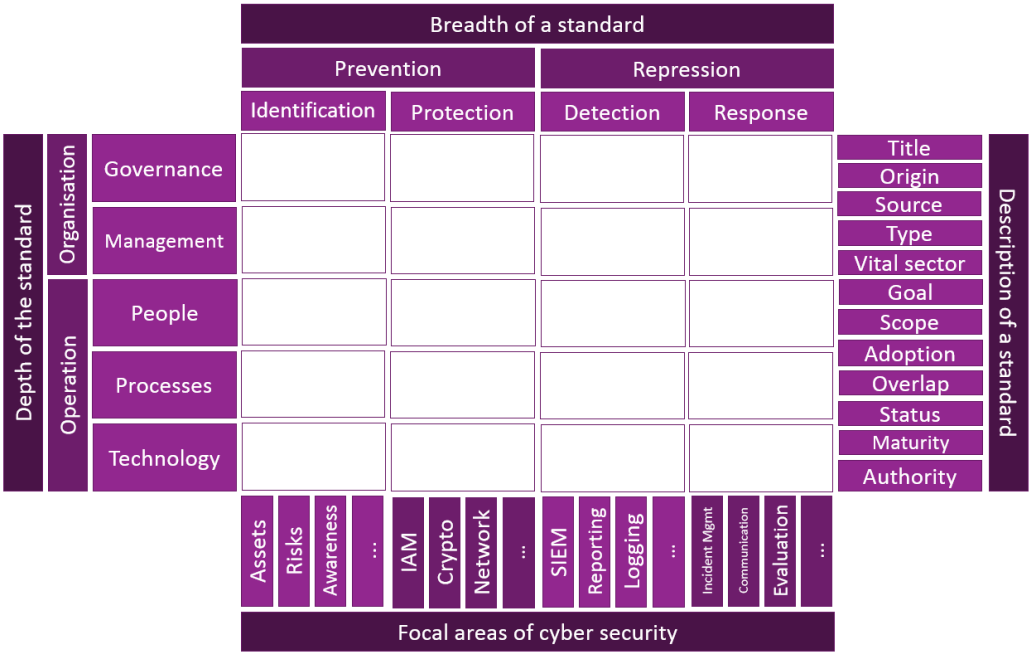

Figure 1: Classification model for cybersecurity standards

CLASSIFICATION OF STANDARDS

The standards for cyber security identified in the inventory were classified according to the dimensions of the classification framework. This indexation was largely completed, for as far as the information available allowed. The cyber security standards classified may now be structurally positioned and compared within the classification framework.

CONTEXTUAL FACTORS

The classification framework does not stand on its own and is embedded in a certain context. Aside from the properties and content of cyber security standards, the context in part affects the selection of a standard. The context consists of influences from without (external factors) and within an organization (internal factors):

- External
  - Law and regulation
  - Technological developments and trends
  - The networks and value chains organizations operate in
  - Societal and individual interests
  - IT-suppliers and software developers
  - Changing methods of cyber criminals

- Internal
  - Business drivers
  - The human factor
  - The cyber security maturity of the organization and its vital sector
  - The impact the implementation of a certain standard would have on the organization
  - Relations between cyber security standardsinsights: statistics and viewpoints

By classifying standards according to the dimensions of the classification framework certain insights could be attained. Statistical information about cyber security standards based on the variables of the

classification framework elucidates for example the availability or properties of cyber security standards. By then combining these variables more detailed viewpoints emerge. For example, the classification framework provides a view of the standards most applied in a certain vital sector. Reflecting on this view could conclude in which goal- or focal areas standardization has not yet been sufficiently adopted or realized. This could be relevant not only for professionals looking to implement standards in their organization, but also for industry organizations or authorities. Other than the domain specific viewpoint explained here, several other viewpoints have been elaborated.

DECISION MODEL FOR THE SELECTION OF CYBER SECURITY STANDARDS

The classification framework may also be applied as a tool to gain decision support information in order to select cyber security standards for measures to be taken to mitigate identified risks. To this end a decision model was developed with which a professional is able to choose a standard in a substantiated way following a few easy steps. The starting point is a risks- and threats analysis from where the professional is guided step by step to one or more positions in the classification framework. Every position yields a number of standards from the inventory and classified information. Based on this information and the contextual situation a professional may select one or more applicable standards.

RECOMMENDATIONS FOR FURTHER RESEARCH

This study inspired a number of recommendations to further develop the inventory of cyber security standards and classification framework:

1. Increase the usability of the classification framework by:
    - Defining a set of common focal areas for cyber security by which standards may be classified.
    - Extending the inventory of standards with more specific standards for the focal areas and classifying them according to the framework.
2. Gathering insights into the practice of cyber security standards in vital sectors by filling out the classification framework for each vital sector. This could be achieved through expert sessions or a questionnaire. The decision model could be helpful in this.
3. Ascertaining the sustenance and relevance of the classification framework and the underlying set of cyber security standards:
    - By considering the presentation of the model, e.g. as an online tool.
    - By considering the governance and maintenance of the inventory and classification.
4. Further explore the influence of contextual factors on the preferences for cyber security standards and implementations thereof:
    - How does the cyber security maturity of the organisation or sector affect the application of standards?
    - How is the quality of cyber security standards assessed? What are the criteria?
5. Gathering knowledge about the actual practice of standards for cyber security:
    - When is the implementation of standards considered successful? What are the criteria and how could they be measured?

CLOSING REMARK

Much progress can be made in the field of cyber security. This is the aim of the second Dutch National Cyber Security Strategy and the European Commission’s cyber security agenda. Insurance against cyber risks in the Netherlands can be reinforced by optimally utilizing cyber security standards. The present inventory of cyber security standards and their classification by means of the classification framework purported here could proof invaluable in achieving this goal.