CYBERSECURITY AUDIT – A CASE STUDY FOR SME

Author : Pascale Dominique, CISA, CRISC, CPA-CA, V-P Certification & Training ISACA – Montreal Chapter.

We need to be flexible in the definition of a Cybersecurity Audit, especially when the mandate is for a “Small and Medium-sized Enterprise” (SME)! Our multidisciplinary team has been involved in security and information technology for more than 25 years. We advise our clients to take advantage of new technologies to maintain their strategic positioning. Our cybersecurity audit mandate with a SME aims at evaluating and proposing recommendations on the state of the network and cybersecurity; guide and advise our client on industry best-practices; and to propose a plan of action to correct weaknesses and vulnerabilities identified and thus reduce the risks related to cybersecurity. Being a member of the ISACA (Information Systems Audit and Control Association) - Montreal Chapter, I seek to provide leverage and added value by presenting a coherent report to the client with technical recommendations supported by standards of good practice. This will help the SMB business leaders understand the action plan, which is not always easy!

When such is the case, we will use best practice guides developed by ISACA to address the particulars of SME’s in conjunction with the National Institute of Standards and Technology (NIST)[1] Cybersecurity programs which promote the development and application of innovative and practical technologies and methodologies for security and improvement of critical cyber security infrastructures.

FIRST PART – USE OF CYBERSECURITY GUIDES

The cybersecurity guides for SMEs[2] proposed by ISACA are essential resources. Aligned with the COBIT5 standard, these guides address the needs of the SME whose technical resources and budgets are often limited.

The "Cybersecurity Guidance for Small and Medium-sized Entreprises" guide first defines the different categories of SMEs and then proposes 8 principles and 55 guidance clauses (requirements / controls). Each clause receives a "Critical" "Severe" or "Important" audit rating, identifying a cybersecurity risk level for an SME, see **Table 1**.

[1] NIST, *Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity V1.1*, USA 2017

[2] ISACA, *Cybersecurity Guidance for Small and Medium-sized Enterprises*, USA, 2015
ISACA, *Implementing Cybersecurity Guidance for Small and Medium-sized Enterprises*, USA 2015
ISACA, *Transforming Cybersecurity*, USA, 2013

Audit Rating Explanation	
Audit Rating	**Explanation**
Critical	Major impact or risk to the enterprise, potentially endangering the existence of the enterprise. Impacts and risk may be financial, operational, reputational, legal or of any other kind.
Significant	Significant impact or risk to the enterprise, with potentially wide-ranging consequences within the business year.
Important	Impact or risk to the enterprise that goes beyond the tolerated levels of impact and risk, as defined by senior management

Table 1- Audit Rating Explanation

Each requirement is assigned with one of the audit rating. **Table 2** presents an example of some of the requirements that emerged while in assignment.

Auditable Cybersecurity Requirements		
Cybersecurity Guidance Clause (CGC)	**Requirements/Controls**	**Audit Rating**
1	Documented cybersecurity governance rules	Critical
4	Documented cybersecurity strategy	Significant
11	Documented procedures and management practices for cybersecurity	Important
21	Documented information asset classification, cybersecurity risk and threats	Significant

Table 2 - Auditable Cybersecurity Requirements

Once our tests and analyzes are completed, we develop recommendations for the identified gaps, weaknesses, or vulnerabilities and prioritize them from 1 to 3. By matching each of our recommendations to one or more of the guide's clauses - see some examples at **Table 3 - Mapping of the requirements and the recommendations**, we add consistency to the report.

C.G.C.	Requirements/Controls	Audit Rating	Recommendations	Priority
1	Documented cybersecurity governance rules	Critical	R1	2
34	Secure configuration of logical points of entry	Critical	R5-R6-R9	1
37	Malware defense mechanisms	Critical	R7	3
38	Boundary defense mechanisms	Critical	R3-R4-R5-R6-R9	1
44	“Need to know” and “Least privilege” principles documented and in evidence	Critical	R8	3
4	Documented cybersecurity strategy	Significant	R1	1
21	Documented information asset inventory/ Documented information asset classification, cybersecurity risk and threats	Significant	R2	1
23	Identified critical IT services and applications, critical IT infrastructures and third party products and services	Significant	R2	2
24	Adequate extent and detail of cybersecurity architecture, size and complexity	Important	R3	2
25	Adequate skills and competencies of cybersecurity staff	Significant	R2	1

Table 3 - Mapping of the requirements and the recommendations

Finally, we will map the proposed recommendations and controls-oriented clauses, which are the minimum requirement criteria for SMEs. **Table 4 – Summary of recommendations by priority and rating**, is an example of the result obtained.

Priority	Audit Rating	No recommendations	Recommendations	Requirements/Controls	C.G.C.
1	Critical	R5	Refresh and review the routers configuration	Secure configuration of logical points of entry	34
		R6	Firewalls		
		R9	Protect against malware softwares		
		R3	Complexity of network	Boundary defense mechanisms	38
		R4	Wi-Fi Network		
		R5-R6-R9	Refresh and review the routers configuration /firewalls / Protect against malware softwares		
2	Critical	R5-R6-R9		Secure configuration mechanisms for hardware/ applications and software	31
2	Significant	R4-R5-R6-R9		Secure configuration mechanisms for network devices including third party devices	33
2	Significant	R4-R5-R6-R7-R9		Identified vulnerabilities	35
1	Significant	R1	No formal documentation regarding security policies and principles	Documented cybersecurity strategy	4
2	Critical			Documented cybersecurity governance rules	1
2	Important			Documented procedures and management practices for cybersecurity	11

Table 4 – Summary of recommendations by priority and rating

Table 4 serves as a basis for facilitating discussion and decision-making on the action plan for implementation of proposed recommendations and corrective actions to be taken to internal controls.

Part Two – Implementation of recommendations and maintenance of critical Cybersecurity infrastructures

The proposed action plan will maintain the confidentiality, integrity and availability of the systems, considering three major axes: 1- good governance, by aligning IT objectives with business goals, 2- risk management deemed acceptable in the achievement of established objectives and 3- the proper use of company resources. To achieve this, our methodology will build on the NIST model for improving critical infrastructure of cybersecurity. This model is adaptive and integrates with the COBIT 5 framework for its implementation. As a Risk-based approach, it is used with a wide range of processes that integrate day-to-day operations by grouping them into 5 major functions as illustrated in **Figure 1- Functions of the NIST CSF Framework Core.**

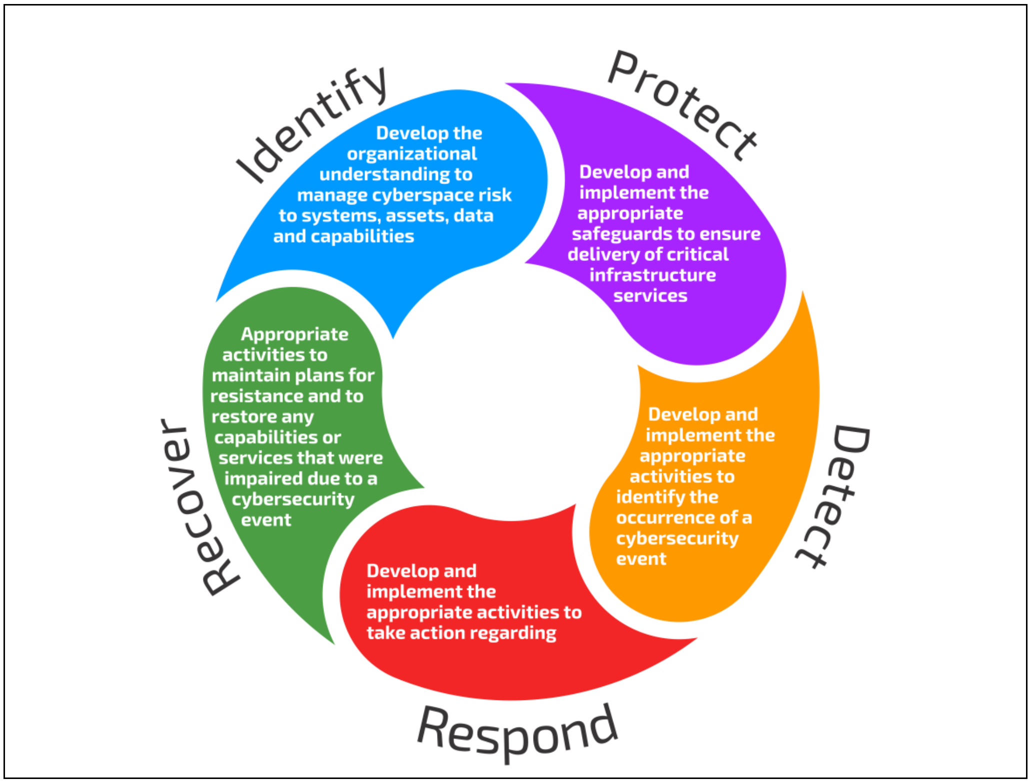
Identify
Develop the organizational understanding to manage cyberspace risk to systems, assets, data and capabilities
Protect
Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services
Detect
Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event
Respond
Develop and implement the appropriate activities to take action regarding
Recover
Appropriate activities to maintain plans for resistance and to restore any capabilities or services that were impaired due to a cybersecurity event

Figure 1- Functions of the NIST CSF Framework Core

At a high level, these functions allow:

- Identification of critical assets of the company;
- Protection of the data they hold;
- Detecting anomalies and incidents in systems;
- The response to ongoing actions, monitoring and improvements to systems and processes when threats or vulnerabilities have been identified;
- Recovery and restore any capabilities or services impaired during a cybersecurity event, follow-ups and actions to be taken for improvement and feedback.

In light of this, the preferred strategy for securing information systems will include measures to protect critical assets at a reasonable cost for the company.

This methodology, which incorporates practices widely used in the industry, is the essence of our professional practice because it allows us to better serve our customers and to enhance the security level of their critical cyber infrastructure.

For more information regarding the cybersecurity audit, visit our website at https://www.connectalk.com/en/it-infrastructure-security/