p-Tools

Productivity methodologies, tools, and techniques

Information security for SMEs: challenges, constraints, and remedies

Organizations depend on information for operations, and protection of information has become a prime need for business continuity and gaining customer confidence and trust. The information security management system (ISMS) of the ISO is an internationally accepted standard that details the preparation/executions required by an organization to protect information assets from internal and external threats. The prime focus is on preserving the confidentiality, integrity, and availability of information deployed by the organization for its business operations. Internal threats refer to error, sabotage, incompetence, etc., while external threats can include natural disasters, terrorism, legal action, network intrusion, etc.

SMEs need to interpret the applicability of the best practices in ISMS vis-à-vis their operations. Factors influencing the interpretation are based upon geoterrain; expectations of customers, potential customers, or interested parties; and core business activities to be sustained. Although standard risks are similar for large organizations and SMEs, handling the risks differs.

Major challenges

1) Insider attack, for example, when the monitoring mechanism is insufficient, operations depend on individual trust, and curiosity could create information breaches.
2) Inability of top personnel to understand the nuances of ICT or falling for the latest jargon.
3) Adherence to legal norms, when monitoring compliance is not systematic.
4) Control of outsourced activity, since dependency on large vendors means that SMEs do not have the last word on security issues.
5) Attrition of trained personnel who then go to multinational/large corporations.

Major constraints

1) Mindset of top management who do not recognize risk.
2) Dependency on ICT, be it a web portal or e-commerce registration for international bidding or tender.
3) Investment in training and competency building. Since SMEs are very sensitive to price, “some” training given might not yield the desired effect. Unfortunately, the fees for training are deemed an expense instead of an investment.
4) Financial inability to protect all entry points (physical or logical), e.g., infrastructure is not available to verify everything coming into the organization like visitors, intrusions, COTS products, repaired equipment, mail, malicious code, and attacks on gateways.
5) Succession planning, when lack of an effective planned dialogue and career mapping leads to an inherent threat of brain drain. The absence of systematic documentation of operations and top management participation in operational functions with less time for strategic thinking also take their toll on developing leaders for key roles.

Remedies

So, what does the ISMS offer? It offers a framework to align best practices, keeping in view the management’s commitment to and direction for the organization. Based on the plan, do, check, act (PDCA) cycle, management systems attempts to induce rigor and institutionalize working practices. This in turn helps to create a culture of learning and implementing new methods to ensure information security for improved organizational sustainability. Managing risk can then be aligned with business growth. The controls put in place provide a shock absorber effect to avoid major negative impacts on the business. The figure shows the conceptual process of continual improvement utilizing the PDCA cycle and an ISMS.

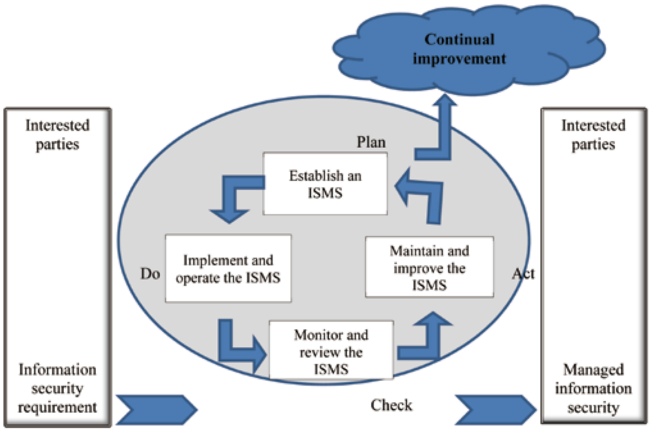
Continual improvement
Interested parties
Information security requirement
Plan
Establish an ISMS
Do
Implement and operate the ISMS
Maintain and improve the ISMS
Act
Monitor and review the ISMS
Check
Interested parties
Managed information security

Figure. The PDCA cycle and ISMS activities. *Source:* ISO 27001:2005

Duggirala S. Prakash received a Bachelor’s in Engineering (Electronics and Telecommunications), along with a Master’s in Business Administration (Marketing). He has more than two decades of experience in quality, manufacturing, maintenance, marketing, safety and security, and management. Prakash is currently employed by M/s. Det Norske Veritas AS, a multinational certification body.