
Key business assurance

# Cyber Security

*Why you need a security program*

# Cyber-security today

Can you imagine a world without access to information? In today's modern world it is difficult to imagine such a situation. This shows how important the access to information has become for businesses and individuals as well. However, more important than access to information is keeping that information secure.

Information security has become a recognized and required business function in today's globalized organizations, when in fact it used to be a "back-office" technical speciality. Rather than just a technology issue, protecting information is a business issue. Today, a vast significance is given to actions, plans and policies that organizations and individuals take to protect information. In today's market where many cyber-attacks and incidents happen around the world, strategic policies, training, awareness activities and audits have proven to be effective to tackle this problem. All these steps make up a strategic effective program called Security Program.

# The meaning of a Security Program

To secure information assets, organizations and individuals should implement comprehensive controls to protect those valuable. The collection of these controls that should be implemented is collectively referred to as a security program.

The security program provides a framework to reach and maintain a desired security level for your organization by assessing risks, deciding how to manage them, and planning how to keep upto-date with security best practices. What such a program enables organizations and individuals to do is to ensure the protection of **confidentiality**, **integrity**, and **availability** of assets, which is central to information security. If all three of these aspects are not protected, the consequences can result in business losses, liability and damage to an organizations reputation.

Introducing a security program is a basis for transforming information security into a proactive action driven by the business leadership. A proactive Information security approach helps organizations to become confident regarding security. It brings structure and governance to the information security function, which can serve as a key element within an enterprise to support its business goals.

Another advantage of this program is that it gives effort to **ensure compliance** to regulations that are related to existing and future information infrastructure. It also enables organizations to make **mature decisions** regarding risk management by delivering information regarding security capabilities in a **business-friendly** perspective.

# Key elements for an effective Security Program

The purpose of the security program is to provide a big picture of how information assets are going be kept secure in an organization, and to describe how every part of the organization is involved in the program.

For a security program to be effective, it takes a transformation of security perception by considering it as an **added business value** rather than an inconvenience and an obstacle to effective operations. To make this happen, the security program should use a top-down approach, where the initiative, support and directives come from top management and go along through middle management until it reaches the operational level.

*After the crucial decisions are taken, the following steps will ensure that the security program is effective:*

1. **Having a Security Officer**

   There should be an officer responsible especially for security program implementation

2. **Assessing Risk Strategically**

   Crucial risks should be defined and followed with up-to-date industry best practices

3. **Policies and Procedures**

   Managing risk instructions should be defined with harmonized procedures

4. **Regal and Regulatory Compliance**

   Ensure that appropriate legal regulations are considered and met.

5. **Continuous Improvement**

   Use follow up actions to improve the program (such as audits and management reviews)

# Conclusion

With the increased regulation of the information infrastructure, continuous cyber-attacks, and the competitive market, the need for an information security program has become crucial. By implementing an information security program, an organization will have a good guide to be compliant with regulations, increase the information safety, and minimize the risks coming from incidents and attacks. This program recommends alignment with industry best practices and at the same time develops such practices.

Zybrstate is a provider of professional training, consulting services and coaching across multiple risk disciplines. Among other training courses, it offers a wide range of information security training courses including ISO 27001, CLPT, CISSP, CLPI, CISA, CISM, SSCP, CHFI, CCFP, CEH, CAP, HCISSP and Data Protection Act Awareness aimed at those who are looking to build a greater knowledge as to how to build an effective and compliant Security Program.

*Want to discuss your state of security? We can always have a coffee!*

***coffee@zybrstate.com***