Midagon Point of View

Pain Points of Cyber Security Improvement

Enterprises today are very dependent on their information systems and data. The IT environment has also become more complex, increasing the risk of information compromise. Cyber security risks are a fundamental type of risk for all organisations to manage. Potential impacts include higher costs, lower revenue, reputational damage, and the impairment of innovation. Cyber security risks also threaten individuals' privacy and access to essential services and can result in life-or-death consequences.

Protecting a company and its information assets requires a holistic approach: various aspects of security controls and compliance need to be understood and addressed to get comprehensive protection:

- **Security and risk management:** Security aims for risk mitigation, and thus, security management practices should be based on threat scenarios and risk analyses. Several options exist for ISMS (Information Security Management System), like the ISO 27001 framework.
- **Information security:** Ensures **information confidentiality, integrity, and availability** in digital and non-digital formats. It also includes information handling and classification principles.
- **IT system security:** Protection of systems, networks, and critical information from various digital attack types.
- **Continuity management:** Linked with business continuity planning, IT continuity ensures that information systems and business processes can be restored in case of significant failure or incident.
- **Data protection:** Ensuring personal information is technically adequately protected, and the process for collecting and handling such data is defined and enforced.

How to get started?

As in all major development activities, top management support and commitment to related budget and allocation of skilled resources is the key to successful cyber security improvement execution. Unfortunately, in many cases, you only get such attention when a significant incident happens, or an external party (a customer or an auditor) triggers mandatory remediation actions.

Security activities are often only seen as cost elements because their benefits come from preventing risks from realising:

- Brand protection (customer trust) in case of an incident
- Critical system downtime due to a security incident
- Leak of business-critical information to competitors
- Violation of legislation like GDPR for personal information protection

Still, in some enterprises, the security organisation is seen as (or even acts like) a party just setting multiple controls to make executing business activities more difficult. Here, the mindset should be changed to see it as an organisation supporting business by protecting the company's critical information and customer trust.

Return of Security Investment (ROSI)

One way of supplying management visibility to measure security cost is using Return of Investment calculation like with other business investment decisions. Return on Security Investment (ROSI) is a metric that quantifies the expected net value of an IT security investment. It is a popular IT management metric in budgeting IT security investments and corporate IT budgets. In the case of cyber security, the Return on Security Investment is focused on risk avoidance and mitigating the negative impact of security-related breaches. Hence, Return on Security Investment focuses on measuring the value of the risk avoided.

ROSI can be calculated using the following formula:

$$ROSI = \frac{ALE * mitigation\ ratio - Cost\ of\ solution}{Cost\ of\ solution}$$

Where ALE is the annual loss expectancy and mitigation ratio tells how much risk is reduced with mitigation actions: If the risk is reduced by 80%, the mitigation ratio is 0.8.

An example of ROSI calculation:

Company X is planning an EDR (Extended Detection and Response) security solution. Each year, there are six security incidents with an average cost (including loss of data and productivity) of 20,000 EUR. The EDR solution is expected to block 90% of these attacks, and its yearly total cost is 50,000 EUR.

The return of security investment in this scenario is

$$ROSI = \frac{(6 * 20{,}000) * 0.9 - 50{,}000}{50{,}000} = 116\%$$

Based on this, the investment is feasible. However, you should remember that only the cost of service is well known in advance, but the individual incident cost and their frequency can only be best estimates.

Security improvement management

Most companies select some well-known framework to build their Information Security Management System (ISMS). The most common framework is ISO 27001, using which you can also get certified on having set up such ISMS. Other common compliance frameworks include PCI-DSS, SOC2, NIST, and HIPAA.

We strongly recommend conducting a gap analysis against the selected ISMS requirements when starting security improvement activities. Various security maturity models can be used to see potential development areas. As a result, a roadmap needs to be created to address found defects in a prioritised order based on the risk level they impose on the organisation.

Cyber security is not only about the technical part executed by the IT organisation, but various service providers, related processes, and human behaviour must also be considered. Therefore, the most effective way is to run the improvement activities as a program or project, linking various stakeholders under the same umbrella.

A properly planned cybersecurity improvement activity must consider the whole company, not only the information security and IT functions. Factories with operational technology and automation technology, as well as business management and supply chain, need to be included in the scope to have the required coverage of the planned activities, as these are often managed independently. Understanding the business and its risk landscape is essential to avoid gaps in planning security measures. This can be achieved by setting up a dedicated program with proper empowerment and steering, covering all relevant stakeholders.

After the scope has been identified, standard professional IT and project management principles need to be followed:

- Management support and commitment, and the availability of active business owner(s) is needed.
- The required resources in numbers and skills are assigned to the project.
- The project content and cost are adequately planned and managed.
- The project team of highly skilled individuals is effectively led.
- The schedule and budget are realistically estimated.
- A larger initiative is properly divided into smaller projects or streams.
- Change management activities are included in the project scope.

Change management in cyber security improvement

It is commonly acknowledged that security requirements cannot be addressed by technical means alone and that a significant part of the protection comes down to the attitudes, awareness, behaviour and capabilities of the people involved. Project management has a close connection, or even a clear role, in communication, supporting business and business management in change leadership and change management activities. Key elements for successful change management include proper stakeholder identification and change impact analysis.

According to studies, up to 85 % of data breaches are caused by human error, so effective change management cannot be underestimated when deploying any security improvement activity. It is not sufficient only to send a notice of a new security measure or policy, but the steps needed shall be included in relevant processes and refreshed regularly.

Good ways to keep employees aware of security topics include:

- Regular information emails
- Information sessions (for each employee role)
- Actively maintained Intranet portal
- Training videos or cartoons
- Email phishing training emails
- Including security topics in the annual employee training curriculum

Midagon

Midagon is a Nordic, independent business and IT consultancy specialising in challenging transformation projects and programs.

We combine extensive information security and risk management understanding, program and project management experience, business domain and technology expertise with 100 % objectivity to help our clients strengthen their cyber security through the following services:

- Information security management
- Business risk and continuity
- Regulatory compliance
- Cyber security improvement project management

Learn more: Midagon Cyber Security services