HOW CAN COMPANIES EFFICIENTLY AND EFFECTIVELY MANAGE CYBER SECURITY INVESTMENTS?

Current Status of Cyber Security Investments

In the last few years, cyber security awareness at top management and board of directors’ level has improved significantly amid daily news on attacks and data thefts. Budgets relating to cyber security have evolved from covering only what is required, with IT security being the first item cut in budget revisions, to “scared” cyber security budgets, where Chief Information Security Office (CISO) requests are usually accepted without a clear understanding of the real benefit in terms of cyber risk reduction for the company. A lack of understanding typically meant that board of directors were not able to challenge the CISO strategy, program and related request of investment.

‘Scared’ cyber security investments are usually defined as having a control and threat-based methodology without a risk-based approach focusing on a company’s critical business information. They are mainly technology-centric investments, derived from market trends and not from real benefits.

Examples of these investments typically include:

- **SIEM implementations used as log collectors**, without security events being analysed in real time and 24/7
- **Very advanced Vulnerability Assessment solutions** without vulnerability management processes (with roles and responsibilities) in place
- **Governance, Risk & Compliance (GRC) solutions** bought without a previously defined cyber risk methodology

From a governance point of view, a cyber operating model is often not clear, with various grey, overlapping areas between different departments (IT, risk, audit, cyber, logistics, HR) and conflict situations that are difficult to resolve.

Risk-Based Cyber Program

The starting point to properly manage cyber security investments is to define a roadmap justified by the mitigation of cyber risk below company risk appetite.

Corporations must protect their critical information in line with the business impact (financial, reputational and compliance) they could have in the event of losing the confidentiality, integrity or availability of data.
The countermeasures defined in the cyber risk roadmap should cover technology, process and organisational aspects, whilst being prioritised by risk and being defined with a cost/benefit analysis.

**Cyber Security Cost Optimisation**

As soon as a program has been defined and implemented, how can the countermeasures and related costs be optimised?

- Companies should evolve from a “classical control” level to an “optimised control” level approach. In other words, they must not only check if a countermeasure is in place but analyse it with a cost/benefit approach and compare it against a market benchmark.
- A well-defined cyber security operating model in terms of services, governance and technology is key for successful cyber cost optimisation.
- An analysis should start with the cyber security services that a company requires. This includes governance, monitoring, engineering, implementation, assessments, etc.
- Following the analysis, the company should cross-check with what currently exists, considering all the departments involved in the service delivery with the possible overlaps, and subsequently, define an optimised target service map.
- Once the service map is defined, analysis must be undertaken into the cyber security organisation in relation to the services previously defined, the size of the company, the market sector and the actual internal capabilities.

**Some important aspects to consider in the cyber governance optimisation are as follows:**

1. **Positioning the Cyber department within the company**: What could be the best positioning of the Cyber department? Should it sit inside or outside the IT department? Or would it sit within the COO organisation, the CRO organisation or just below the CEO?
2. **Cyber security skills**: Audit the current skills across various departments to optimise the number of people in the organisation and the number of possible external suppliers (e.g. managed security service providers)
3. **Cyber department iterations with others**: For example;
   1. IT for security product implementation;
   2. physical security for convergence with logical security;
   3. risk for enterprise risk management,
   4. production in manufacturing environments;
   5. HR for background checks and personal data, etc.
4. Cyber security processes and procedures with roles and responsibilities

Finally, optimisation of cyber security technology could lead to important savings. It is important to be aware of all possible security products within your company, and ensure they are being used effectively. Is the current solution the best solution for your company’s actual needs?

**A&M CYBER SECURITY SERVICES**

A&M helps board of directors and top management to understand, evaluate and effectively manage cyber risks, in order to justify cyber security investments by the reduction of the related business risk below the company risk appetite. Our firm’s suite of capabilities includes the following service offerings. **Reach out to us to learn more.**

- Cyber Security Analysis
  - Quick Cyber Maturity Assessment
  - Cyber Risk Evaluation and Program Definition
  - Cyber Organisation and Skill Assessment
- Cyber Program Execution
  - Shadow Management or Interim Roles (i.e. CISO) to Implement and Govern the Cyber Strategy and the Related Program, and the Target Cyber Organisation
- Cyber Steering Committee
  - Advising CxOs about Cyber Risk Status on a Regular Basis
  - Helping CIO/CISO to Present the Relevant Cyber Data to the Business
- Cyber Incident Response & Investigation
○ Cyber Crisis Management
○ Cyber Incident Root-Cause Investigation
○ Cyber Incident Recovery
○ Interim Management Roles

Source URL: https://www.alvarezandmarsal.com/insights/cyber-security-cost-optimisation

Authors:
Lorenzo Grillo, mailto:lgrillo@alvarezandmarsal.com, +44 778 830 0850