

Changing the Focus – Information Security as a Strategic Business Function

Paul R. Mudgett, CISSP, CISA

Information security has long been considered a technical entity, tied closely with IT operations and struggling to gain recognition from even a tactical perspective. Over the last few years the winds of business value have shifted thanks to increased regulatory obligations and high profile data compromises. This transition has placed information security in a strategic position in some organizations yet in many cases; information security has yet to find a seat at the strategic table.

The barriers to this evolution are twofold. On one side, CEO's, Presidents and Board Members fail to recognize the strategic value in information security. This is not entirely their fault. They have been overexposed to the tactics of fear, uncertainty and doubt...the FUD factor. When the prophecy of the next security catastrophe fails to materialize, the stock in security credibility simply drops. This worn-out tactic to gain a greater share of the budget doesn't suit today's cost justification and benefit-driven corporate environment.

On the other side of the evolution blockade, some Information Security leaders have found it difficult to make the mental transition from a technical point of view to a business oriented position. This frame of mind stalls the growth of information security as a business-valued department placing an artificial ceiling on the potential of information security as a business enabler.

There are many approaches to making this shift however, the following four points may serve to kick start the process for InfoSec leaders and organizations that desire to bring value to the table.

- Understand business objectives by reading and discussing the organizational strategic plan and matching information security initiatives to this plan. Showing that information security can be an enabler and contributor to the business future

brings information security into the same realm as other business oriented departments.

- Drop the technical speak and learn terms familiar with corporate business leaders. Every field has its own jargon however aligning information security with business requires that the security professional speak in terms that business leaders can understand.
- Perform risk assessments. Without understanding the threats and likelihood of damage to your assets, you cannot possibly know where to effectively plan for privacy and security. The goal is to allow CEO's and Presidents to make informed decisions regarding acceptable risk. In the end, those responsible for shareholder value will make the final call on what is acceptable risk.
- Security is becoming more and more metrics-driven. Learn to demonstrate the value of information security by using measurements that make sense. There is substantial legwork involved but thoughtful use of measurements is vital to investment value and strategy development.

With increased regulatory requirements, public scrutiny over the use of sensitive information and increased awareness of the business-security relationship, the role of information security has gained importance. Rather than falling further behind the strategic curve, information security should seize this opportunity by making measured investments and decisions that clearly enable business and then communicate the value information security brings.