



DOI: **10.5958/2249-7137.2021.01149.6**

MAKING INFORMATION SECURITY STRATEGIC TO BUSINESS

S.M.Turdaliyev*; **A.R.Yuldashev****; **I.I.Djo'rayev*****; **T.V.Mamadaliyev******

*Teacher of Kokand State Pedagogical Institute,
UZBEKISTAN

**Teacher of Kokand State Pedagogical Institute,
UZBEKISTAN

***Teacher of Kokand State Pedagogical Institute,
UZBEKISTAN

****Teacher of Kokand State Pedagogical Institute,
UZBEKISTAN

ABSTRACT

This article informs about the the importance of strategies of making business information. As well as security strategic faktors economy in use. Often times, the information contained within these environments is very sensitive and can potentially be put at risk if accessed or changed by an unauthorised user. This lack of security planning creates unnecessarily high costs and project delays. Generally, it costs far less to "build security in" than it does to "bolt it on" at the end. And while the recent economic downturn will certainly drive security teams to focus on finding operational efficiencies, it is important to note that efficiencies alone will not be sufficient to get us out of the economic crisis the world is facing.

KEYWORDS: *Innovation, Business, Information Security, Strategy.*

INTRODUCTION

Information security is undergoing a critical transformation. Traditionally viewed as a necessary evil or worse, a hindrance to business advancement, now, more than ever, it is critical that security strategy aligns to business priorities and enables innovation. And while the recent economic downturn will certainly drive security teams to focus on finding operational efficiencies, it is important to note that efficiencies alone will not be sufficient to get us out of the economic crisis the world is facing. Political and business experts agree that business

innovation is key to the return of global economic stability and growth. And information security has a critical role to play in the drive toward innovation.

Why? Because at the heart of many critical innovations is the secure and fluid exchange of information. We are an information-centric economy, heavily dependent on the information we create and share; and we find ourselves in an age of digital warfare where that information is put at risk everyday. The goal of the security organisation must be to enable the business to safely manage risk to gain maximum business advantage.

Security is a Balancing Act. What does this mean for today's businesses? It is important to note that how organisations innovate has changed over time from internal groups working side-by-side creating new products in a lab to geographically dispersed teams collaborating across organisational and physical boundaries. Innovation now requires open collaboration, direct interaction with customers, tighter integration with partners, and the incorporation of external talent and resources.

It demands sharing intellectual property, infrastructure and ideas, while at the same time safeguarding trademarks, copyrights, and patents. Forward-thinking security leaders have made tremendous progress in driving tighter linkages between business innovation goals and security actions. A critical element has been taking a more structured and strategic approach to organisational risk assessment.

Without the right security strategy, business innovation could be stifled or put the organisation at great risk. But because the business and security teams operate in separate silos, security is often applied as an afterthought. This lack of security planning creates unnecessarily high costs and project delays. Generally, it costs far less to "build security in" than it does to "bolt it on" at the end. It is imperative that security teams understand key business priorities and ensure that they are brought into the planning process early. To do this they will need to speak the language of business, not security.

Setting Risk Management in Motio. Recently, there has been a growing recognition of the need to take a risk-based approach to security. Different organisations are at different stages along this progression, based not only on how they view information security and its importance to the business but also on the maturity of their enterprise risk management program. There are some preconditions that are essential to the success of any security team's efforts.

First, the organisation must already be using the construct of "risk" in how they make investment and operational decisions. Some organisations may not have the culture for a risk-based approach as their strategy is still too tactical or "targeted opportunity" focused. The other key prerequisite is that there has to be sustained attention from the top. If there is no attention for enterprise risk management or at least some notion of assessing risk at the board or senior leadership level, then trying to be effective in information risk management is likely beyond the organisation's current capability.

A key component of building a security program that enables innovation is moving from "information security" to "information risk management (IRM)." IRM must incorporate the idea that information security is striving for an acceptable level of risk. The goal is to match risk exposure to risk appetite, not wipe out all risk. Having specific expertise in information security per se is still a crucial part of the program as it is essential for determining the optimum security

controls. Managing information risks must be conducted in a way that is meaningful to the business and is based on how other categories of risk are discussed and calculated.

So IRM must be integrated into the enterprise risk management framework. As an example, let's look at risk management and innovation in the context of data loss prevention. Many organisations are increasingly using Web-based collaborative tools to facilitate information and knowledge sharing among various user groups in order to improve productivity and eliminate the duplication of efforts.

Often times, the information contained within these environments is very sensitive and can potentially be put at risk if accessed or changed by an unauthorised user. Determining what data is most sensitive or at highest risk and identifying where it resides is the first step in preventing enterprise data loss. But understanding risk becomes important when it's time to implement the controls to prevent data loss. This is the step where security professionals are challenged to establish what level of risk they are willing to accept without stifling the innovation process.

Each organisation must qualitatively and quantitatively answer the following: How does an organisation measure risk? What kinds of controls should be implemented to protect the data? Who should be able to have access or make edits to the document? What kind of actions should be allowed (i.e., can it be printed or saved to external media)? And finally, what kind of action should be taken if the data is inadvertently accessed, changed or an attempt is made to send it (i.e., notification, quarantine, encrypt)? Determining a reasonable risk threshold while avoiding unnecessary disruption to your employees is a delicate balancing act.

The Time Is Now. The time is now for security professionals to establish themselves as a "trusted business partner." Security practitioners need to move beyond applying the security technology du jour to meet the latest audit, and instead focus on supporting key business initiatives while meeting compliance objectives.

Security needs to be framed in a business context. Staying ahead of the business and being prepared to promote security as an accelerator rather than an inhibitor will ensure that security has its rightful place at the innovation table.

LITERATURE

- https://en.wikipedia.org/wiki/Silicon_Valley.
- <http://www.kylbakov.ru/page110/page144/index.html>
- <http://tehprog.ru>