

PMG 663

Managing IT and Cyber Risks in Supply Chains

Lecture 3

Prepared by
Dr. Badur elgasim

Learning Objectives

IT Risks and Cyber Risks

supply chain critical points

Managing IT and Cyber Risks in Supply Chains: A Practical Framework

Practical Evidence from a European Sample of Companies

IT Risks and Cyber Risks: Real Threats for All Supply Chains

Global trends, such as digitalization and servitization, have caused an evolution in all conventional supply chains whose structures have switched from a “web of disconnected islands” to a network of interconnected processes, which are strongly oriented toward flexibility, efficiency, and resilience

Internet platforms assure operational benefits, such as cost reduction, inventory pooling, postponement, a reduction of the bullwhip effect, and shorter lead times, to allow for faster information sharing across different organizations. For example, supply chain leaders such as Wal-Mart, Procter and Gamble, have achieved great benefits from their investments in Information Technology (IT) tools such as the Enterprise Resource Planning (ERP). In particular, these companies have improved their performances in demand planning and scheduling production, which have created better coordination with their key supplier

However, the use of IT tools and Internet platforms generates new forms of supply chain vulnerability and new risks, which may affect the supply chain's continuity and performance. Managers should recognize these new threats as critical issues that may exacerbate the other supply chain risks throughout interdependencies

, supply chain managers need to focus more attention on the management of all risks that may be generated by IT tools, such as ERP or any vertical software, and external Cyberspace

“Cyberattacks” to be events such as fraud, identity or intellectual property theft, and political statements made by hacktivists.

IT as a tool and an enabler of seamless and real-time interconnectivity across the entire network. Part of the literature considers the two risks related and even occasionally exchangeable. Both are not easily predictable, and they always imply a violation of three key properties: confidentiality, availability, and integrity

IT as the foundation of Cyberspace , while others consider it a mere infrastructure, where hardware, software, and external data represent “Cyber assets”. Cyberspace is typically considered an external environment with low entry barriers, which have an ambiguity characterized by a certain risk exposure

In practice, IT risks seem strictly technical: they stem from failures of ERP/IT systems and impact only on the flow of information itself. Here, the control of technical features and procedures plays a key role in assuring information security. Cyber risks go beyond mere IT disruptions; they are linked to human Cyberattacks, where hackers intentionally access an organization or a network with the goal of either gaining an economic advantage or causing sabotage.

These actions are typically linked to cyber bullying, cyber terrorism, or political issues . In 2014, found that, while IT and cyber-related breaches are occurring with growing regularity, executives perceive that they are not quickly responding with adequate tools .

In the Global Risk Management Report (Aon 2015), “Cyberattacks” were listed in the top 10 threatening risks for organizations and network

Despite these perceptions, cyber security and IT security remain the areas of risk management with the largest gap between the level of threat and the amount of resources invested. Therefore, supply chain managers should carefully focus on two critical points:

1. Information security should not be considered as a technology investment itself. Instead, decisions should be made that involve all the actors in the supply chain, create an awareness about IT and cyber risks, and define clear procedures to identify these threats to protect the supply chain from these vulnerabilities.

2. Managing IT and cyber risks may increase the overall performance, which will augment the sharing of information and collaboration as well as the efficient management of processes across the supply chain.

Managing IT and Cyber Risks in Supply Chains: A Practical Framework

a supply chain risk management framework that may guide managers to assess and manage IT and cyber risks in protecting supply chain processes. We addressed key risks, such as IT failures, piracy and thefts, product shortages, safety and security, inventory levels, and supplier dependence, which may significantly affect strategic, financial, and operational performances of all actors in a supply chain

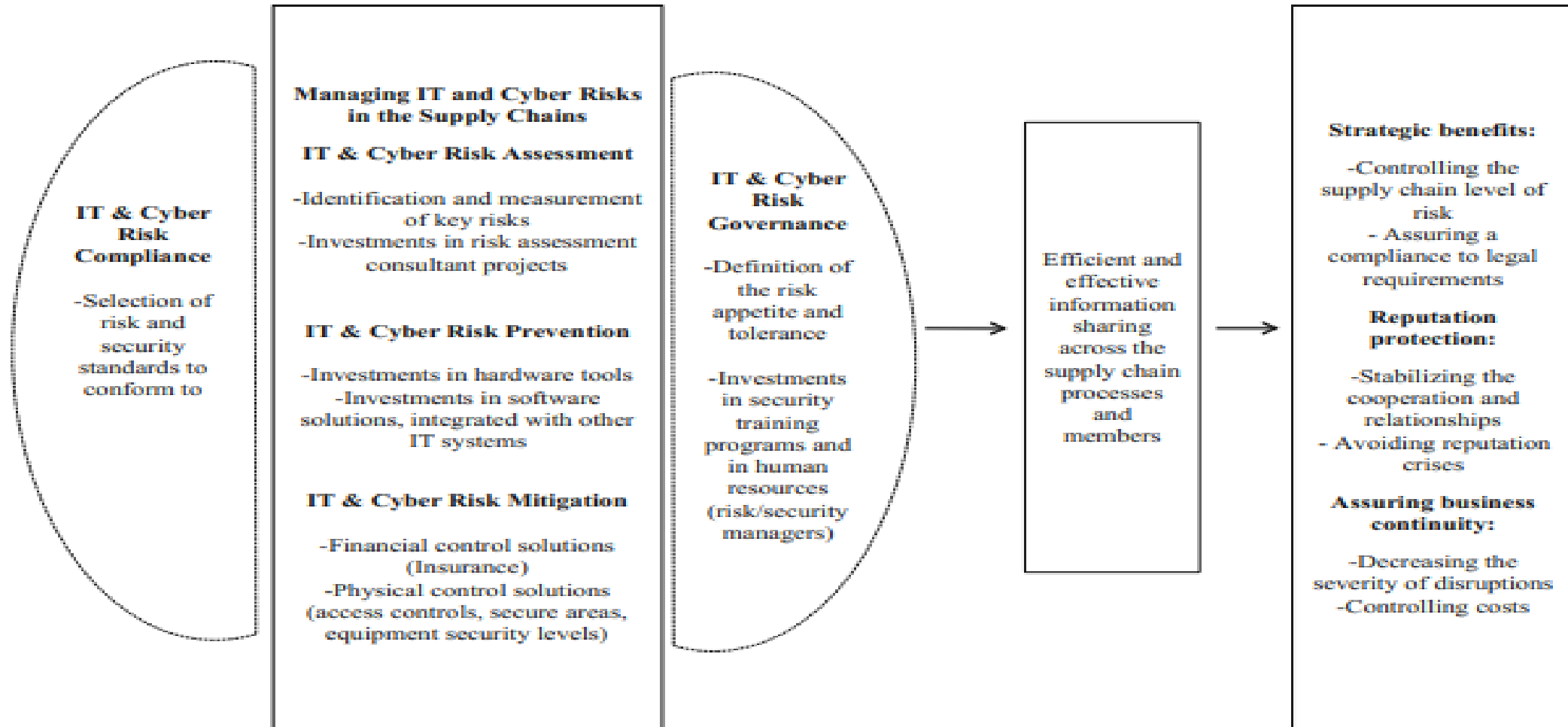


Fig. 5.1 A framework for managing IT and cyber risks in supply chains

key steps of a risk management process (risk assessment, risk treatment, risk governance, and risk compliance) should be adapted to IT and cyber risks. A robust IT and cyber risk management program may protect the strategic goals of the supply chain, preventing business disruptions and protecting the reputation of all actors involved

Firstly, managing IT and cyber risks would have the strategic benefits of enhancing the firms' capability to guarantee a tolerable level of overall risk for all actors involved and consistently do so within their real risk appetite. Thus, managers should monitor if and how IT and cyber risks may threaten relevant assets and relationships with upstream and downstream supply chain partners. **Secondly**, IT failures, piracy, thefts, and Cyberattacks are listed among the major causes of reputation crises and losses of reputation value. Protecting the supply chain against those risks requires stable relationships amongst supply chain members and fostering collaboration.

Thirdly, IT failures and Cyberattacks may cause business interruptions, which in turn may damage suppliers' and customers' operational and financial performances. The risk management process should therefore start with a careful assessment of the sources of IT and cyber risks amongst all supply chain members. In companies that lack awareness of these risks, the role of the “channel captain” is essential. These supply chain leaders should, for example, lead supply chain risk management projects or include them in their contractual agreements or sourcing strategies' ad hoc requirements regarding investments in IT and cyber risk consultancy projects.

After the assessment (identification, measurement, and evaluation) of these risks, each supply chain member should decide the nature and amount of investments in risk prevention strategies, such as investments in hardware and software, which they plan to implement. Risk mitigation strategies reduce the severity of disruptions, control costs, and assure continuity of supplies. Risk mitigation comprises both financial controls (IT and cyber risk insurance programs) and physical controls (investing in access control, secure areas, equipment security levels).

This framework offers a holistic risk management process, in which the abovementioned strategies, processes, technologies, and human resources should be aligned in coherence with the governance of each organization and of the supply chain as a whole. Several variables will influence the implementation of the risk management process such as the position of the supply chain captain (i.e., a manufacturer or a retailer),

strategic priorities (i.e., efficiency vs. responsiveness), the industry/markets (there are different security standards to conform to, such as ISO/IEC 27001:2013, depending on the sector/markets), and organizations' dimensions. The final result should be a supply chain where the actors share more information throughout the whole process, which guarantees strategic benefits, reputation protection, and business continuity

Recent literature has poorly investigated the perceptions and decision-making processes regarding the management of IT and cyber risks within the supply chain. This led us to conduct an empirical investigation of European organizations that rely on security and risk management standards in order to choose the drivers of systematic IT and cyber risk management (risk assessment, risk prevention, risk mitigation, risk compliance, and risk governance)

To investigate whether or not the perceptions and management of these risks vary, depending on the industry, performance, and globalization choices of organizations, it's considered heterogeneity with regard to the industries they operate in, their size, and their level of internationalization .The sample involved several European companies including: one small, local company, with a revenue under €1 million, which had between 10 and 100 employees; seven medium companies, with revenues between €1 million and €500 million, less than 50 thousand employees, and that represented various interests internationally; and seven large companies

Risk management process	Main references
<i>Risk assessment</i>	
• Identification and measurement of key risks such as - Inadvertent breaches - Deliberate attacks - Asset thefts - Equipment failures - Backup failures - Data thefts - Site disasters - Copyright infringements • Presence of a dedicated budget for IT security management • Investments in risk assessment consulting projects	Yildirim et al. (2011) Biener et al. (2015) Järveläinen (2013)

Risk prevention

- Investments in hardware tools
- Investments in software solutions integrated with other IT systems

Ifinedo (2012)
Järveläinen (2013)
Yildirim et al. (2011)
Biener et al. (2015)
Boyson (2014)
Silva et al. (2014)

Risk mitigation

- Financial control solutions (insurance)
- Physical control solutions (access controls, secure areas, and equipment security levels)

Biener et al. (2015)
Silva et al. (2014)
Feng et al. (2014)
Yildirim et al. (2011)

Risk governance

- Defining the organization's risk appetite and tolerance
- Investments in ad hoc training programs in security
- Investments in organizational human resources (risk manager, security manager, etc.)

Järveläinen (2013)
Yildirim et al. (2011)
Boyson (2014)
Ifinedo (2012)
Johnston et al. (2010)
Biener et al. (2015)

Risk compliance

- Perception of the organization regarding exposure and vulnerability toward IT and cyber risks
- Risk appetite of an organization

Yildirim et al. (2011)
Ifinedo (2012)
Bulgurcu et al. (2010)
Feng et al. (2014)
Biener et al. (2015)
Boyson (2014)

Some evidences from our research are summarized in Table 5.2. The sample revealed that managing IT risks and cyber risks positively influences reputation toward both the upstream and downstream actors of the supply chain. However, the commitment to managing these risks and protecting reputation varied by the dependence of the supply chain under observation: IT and cyber risk management toward the upstream supply chain was almost non-existent, while a higher commitment was seen toward clients and customer . In fact, managers perceived breaches to private and personal information as less tolerable than threats to business-to-business partners

Strategic and operational advantages related to careful IT and cyber risk management currently lack acknowledgement. Thus, managers usually neither stipulate contractual agreements with key suppliers nor implement systematic plans for disaster recovery, business continuity, or the backup of sensitive data. Moreover, there is a low commitment at the corporate level: risk and security managers show a greater awareness about IT and cyber risks, while top managers do not prioritize their management. The consequence is a scarce effort in building a deeper awareness among employees through systematic training.

Regarding risk assessment, IT and cyber risks were systematically assessed by more than half of the sample, who also had a dedicated budget. However, the identification and measurement of key risks appeared to be far from effective: three out of four of the respondents had faced some IT and cyber breaches in the last 24 months.

Investments in risk assessment consulting projects were low for the majority of larger, multinational organizations, which used consultancy “on demand” for testing protection systems (penetration intrusion test), disaster recovery, and backup systems

Regarding risk treatment, mitigation strategies were widely used, even if the majority was exclusively dedicated to IT risks. More than half of the sample had a budget solely dedicated to software, hardware, insurance, physical entry controls, secure areas, and equipment security levels.

Interestingly, managers appeared genuinely convinced that effective IT and cyber risk management was possible solely through these types of investments

Risk prevention rarely accounted for ad hoc investments by most of the organizations.

Thus, they seemed somewhat disoriented by the breaches from which they suffered; a third of the sample admitted that companies tend to be high-risk takers, with a dramatic number of IT and cyber breaches discovered roughly six months after the fact

In general, risks were assessed by only one out of three organizations. Interestingly, the majority of them were medium and small companies, which invested in protection, disaster recovery, and backup consultancy services.

The only exception to this trend was represented by multinational operations in the financial and oil industries, which invested significantly in risk assessment consulting projects. However, they often required consultancy services exclusively to assess cyber risks and rarely for IT risks

Efforts in IT and cyber risk prevention were performed systematically by all the multinational companies and by the small organization, which operates in the software industry.

As mentioned earlier, roughly all the sampled companies implemented systematic mitigation strategies. The only striking exceptions were the small organization and all those operating in the healthcare industry

The majority of the medium and small companies perceived low exposure and vulnerability toward IT and cyber risks, while risk appetite was declared to be very low throughout all companies and industries.

Roughly all the companies invested in ad hoc training programs in security, but they were only directed toward the risk and security managers, never to all the employees. In general, finance and high technology industries showed the most careful and systematic IT and cyber risk management processes, while the healthcare sector implemented only occasional measures

The pervasive use of Internet throughout the entire value chain may assure significant advantages to organizations, particularly in terms of resilience.

To investigate how companies in practice perceive IT and cyber risks and whether they include them in their decision-making process, we conducted an exploratory survey among different European companies, leaders in their industries.

The findings show a lack of awareness at different organizational levels. Employees seem to be unprepared to deal with these risks and with their effects onto processes and operations.

From the top management perspective, managers seem to dedicate insufficient efforts and investments particularly in IT and cyber risk mitigation strategies, mainly using reactive approaches instead of proactive ones

The proposed risk management framework seems to fill an existing gap in the literature, addressing how systematic IT and cyber risk management may enhance the ability to share information and better manage supply chain processes. From a practitioner perspective, the framework addresses those risks—such as IT failures, piracy and thefts, product shortages, safety and security, inventory over-stocks, and supplier dependence—which may significantly affect supply chain performances

. In practice, this approach may guide managers to formally assess and manage IT and cyber risks in order to protect supply chain processes. Moreover, the framework promotes a formal mitigation plan to update systematically, in order to respond to IT and cyber risks, considering the time pressure these new threats impose to all the actors of the supply chain

These risk management process should be constantly supported by strong commitment from top management, especially in conforming to the ad hoc security standards and the definition of the real risk appetite and tolerance of the company.

Managers should also be engaged in promoting an overall “IT and cyber culture” transversally in the entire supply chain, because IT and cyber risks represent significant threats for both the upstream and downstream supply chain.

Reference

Supply Chain Risk Management Advanced Tools, Models, and Developments

By: Yacob Khojasteh

-ISBN 978-981-10-4106-8 (eBook)

Chapter 2



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

