IMPROVING SUPPLY CHAIN SECURITY

FOR BETTER BUSINESS GOVERNANCE

Supply chains magnify enterprise risk. This paper examines the common risks presented by third party suppliers, the options available to organizations to streamline assessment programs, particularly vis-à-vis cybersecurity, and how to approach supply chain security risk management within a GRC framework.

Portia Mills, Director of Marketing, Modulo
Barrett Hightower, Consultant for Supply Chain Risk

Improving Supply Chain Security for Better Business Governance

July 22, 2014

EXECUTIVE OVERVIEW

Supply chains magnify enterprise risk. A wide array of potential threats comprising an enormous diversity of risks lie buried within different layers of every company's supplier network. No company is immune. Some of these threats manifest far upstream while others lurk just outside an organization's operational core. Companies need insight into which risks to mitigate and which to absorb.

Today's major global organizations with hundreds of locations and thousands of employees and suppliers must efficiently address risk. Governance, risk, and compliance (GRC) management provides a sound structure:

- ✓ Identifying redundancies as well as gaps in complex compliance requirements,
- ✓ Accurately managing and reporting risks and threats across the enterprise and extended network of third-party suppliers, and
- ✓ Achieving efficient governance of all operations

Effective governance and threat mitigation is nearly impossible without enhancing enterprise risk management to include both

- ✓ Vendor risk management, and
- ✓ Supply chain security management

The common silo approach to vendor risk and supply chain security leaves organizations wide open to threats they "should" know about. More importantly, evaluating risk from the perspective of cyber security or physical security alone ignores an important opportunity to identify and leverage synergies between the two approaches.

Tackling supply chain security within a GRC management program allows organizations to automate processes and improve visibility into operational risk. This paper examines the common risks presented by third party suppliers, the options available to organizations to streamline assessment programs, particularly vis-à-vis cybersecurity, and how to approach supply chain security risk management within a GRC framework.

Some examples of risks buried in the supplier network

- ✓ Rare earth mine uses child labor to cut costs
- ✓ Manufacturer experiences a quality assurance failure in a critical subcomponent
- ✓ Shipping company experiences major losses due to storms
- ✓ Payroll management system experiences an IT vulnerability
- ✓ Heating/cooling vendor gets **hacked** by cyber criminals

THE PROBLEM: EXTENDED NETWORK, EXTENDED RISK

Third parties, vendors, and supply chains are all fashionable terms for all the business -to-business relationships upon which companies rely day to day. For a grocer, a food distributor is a vendor. For a computer maker, a Malaysian chip manufacturer is a vendor. In an energy company, an important vendor is the company providing contract workers. In each of these cases, and countless thousands more, third parties represent critical assets of business operations.

The network of vendors – product suppliers, brokers, logistics operators, services providers – through which products move and across which companies communicate, create a complex physical and virtual supply chain. In fact, the more governments and businesses rely on electronic media for record-keeping, data-sharing, and other communication, the more interdependent these supply chains become. However, as essential as they are to efficient and low cost operations, third-parties also introduce risks and complicate an already-difficult process of risk management.

> **"Without proper insight, organizations may find themselves the unsuspecting 'sharer' of transferred risk from a supplier."**

According to ISO 31000, risk management involves the identification, assessment, and prioritization of risks followed by coordinated and resourceful efforts to minimize, monitor, and control the impact of future events. Options for risk treatment include avoidance, reduction, sharing, or retention. Organizations can opt to retain (plan to financially absorb) certain levels of unanticipated third-party risk but, without proper insight, may find themselves the unsuspecting "sharer" of transferred risk from a supplier.

While risk transfer affects the whole enterprise, companies often manage supply chain security risk and compliance separately from other compliance areas – both in internal corporate policies and in external requirements, such as those set by the U.S. Customs-Trade Partnership against Terrorism (C-TPAT) program, Canada's Partners in Protection (PIP) program, or the Authorized Economic Operator (AEO) Safety and Security Certificate. This creates major gaps in security and risk management. Piecemeal compliance tactics drain resources, risk vendor fatigue and, perhaps most importantly, make it impossible to leverage security gains across multiple business areas and to address advanced threats. Ensuring a minimum level of compliance – checking of boxes – to laws or policies lets organizations dictate how they will address and "treat" risk.

At a high level, effective risk management requires a single vision, call it "governance," that spans departments, geographies, and compliance requirements. At the business-process level, easier, more integrated information gathering and reporting procedures ensure higher participation in governance-related activities and improve access to accurate information.

Manage the relationship between physical and cyber security

A medical center arranged to have a vendor pick up documents and shred them prior to disposal. Apparently, an actual "pickup" truck was used, because the files ended up all over the roadside instead. "It looked like a blizzard of white paper had struck the area," according to one witness. These were old medical records with all manner of protected information. When people found them and called law enforcement, an inmate crew doing regular trash pickup in the area was sent to retrieve these sensitive documents. And that's the sound of the men working on the "cha-ching" gang.

- Example from the Verizon 2014 Data Breach Investigations Report

ISO31000: Risk Management Principles and Guidelines

- ✓ Increase the likelihood of achieving objectives;
- ✓ Encourage proactive management;
- ✓ Be aware of the need to identify and treat risk throughout the organization;
- ✓ Improve the identification of opportunities and threats;
- ✓ Comply with relevant legal and regulatory requirements and international norms;
- ✓ Improve mandatory and voluntary reporting;
- ✓ Improve governance;
- ✓ Improve stakeholder confidence and trust;
- ✓ Establish a reliable basis for decision making and planning;
- ✓ Improve controls;
- ✓ Effectively allocate and use resources for risk treatment;
- ✓ Improve operational effectiveness and efficiency;
- ✓ Enhance health and safety performance, as well as environmental protection;
- ✓ Improve loss prevention and incident management;
- ✓ Minimize losses;
- ✓ Improve organizational learning; and
- ✓ Improve organizational resilience.

- ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees… ISO 31000 was prepared by the ISO Technical Management Board Working Group on risk management. – From ISO 31000:2009

BETTER GOVERNANCE: OPPORTUNITY WITHIN SUPPLY CHAIN SECURITY COMPLIANCE

Global Supply Chain Security in Customs Organizations

In 2005, the World Customs Organization SAFE Standards to Secure and Facilitate Global Trade (WCO SAFE) set a foundation for strengthening 1) customs-to-customs networks and 2) customs-to-business partnerships. Nearly a decade later, benefits are materializing across customs and partner organizations. Governments are sharing more resources and data and trusted trader networks are expanding through the implementation of mutual recognition agreements (MRAs), which aim to reduce redundant audit processes. The customs-business partnerships are providing regulators with information that improves targeting, advanced screening, and clearance streamlining.

For U.S.-based partner organizations, the voluntary Customs-Trade Partnership Against Terrorism (C-TPAT) program recommends the minimum following steps for identifying risk and assessing international supply chain security:

- ✓ Mapping cargo flow and identifying business partners (third parties)
- ✓ Conducting threat assessments on:
  - Terrorism
  - Contraband Smuggling
  - Human Smuggling
  - Organized Crime
- ✓ Assessing vulnerabilities in accordance with C-TPAT minimum security criteria
- ✓ Preparing action plans
- ✓ Documenting processes (on going)

Recommendations for similar programs all over the world are very similar.

Regulators' minimum standards for import and export supply chain security are true to the definition of "minimum" but share commonalities across national and regional programs that continue to come online and attract members. The number of countries adopting the AEO Safety and Security Certificate is rising. The European Union, Japan, South Korea, Dominican Republic, Brazil, Argentina, and a number of other, especially Asian and Latin American customs organizations, now offer certificates and confer benefits. The list of programs that CBP mutually recognizes is growing too, including a pending agreement with Mexico's New Scheme of Certified Companies (NEEC). Mutual recognition agreements that do not involve the United States include the MRA signed in May 2014 between the EU and China.

Government-sponsored programs are currently extremely similar, identical in many cases; however, even under mutual-recognition frameworks, national-level requirements create redundancies for private-sector participants. The same mutual recognition network that is helping to reduce governments' workloads should translate into an opportunity for the private sector to streamline compliance with different-but-similar regimes. Cross-mapping these requirements offers participating organizations one opportunity to reduce redundancies in supply chain security program compliance.

Customers-Trade Partnership Against Terrorism Goals vs. Enterprise Risk Management Goals

Customs and Border Patrol C-TPAT Goals

- ✓ Ensure that C-TPAT partners improve the security of supply chains pursuant to C-TPAT security criteria
- ✓ Provide incentives and benefits to include expedited processing of C-TPAT shipments to C-TPAT partners
- ✓ Internationalize the core principles of C-TPAT through cooperation and coordination with the international community
- ✓ Support other CBP security and facilitation initiatives
- ✓ Improve administration of the C-TPAT program

Partner's Security Goals

- ✓ Improve security of supply chains pursuant to C-TPAT security criteria as part of broader supply chain security and enterprise security goals
- ✓ Track and report on return on investment for C-TPAT compliance, to include expedited processing of C-TPAT shipments
- ✓ Leverage internationalization of C-TPAT cooperation and coordination to bring international business units and vendors into compliance with enterprise-wide security program
- ✓ Report tangible and intangible benefits from support received by CBP and related security and facilitation initiatives
- ✓ Leverage C-TPAT and related programs to improve administration of enterprise security program

INTEGRATING SUPPLY CHAIN SECURITY INTO GOVERNANCE OBJECTIVES

Supply chain security risk management is interdisciplinary by design. Customs' minimum-security requirements require and leverage a variety of practices business already employ. Canada's PIP program and the AEO programs include policies and practices around business continuity and disaster response. The AEO programs also address secure export policies and practices, and the U.S. program is moving in this direction. Yet all too often, organizations allow involved departments such as human resources, IT, and policy teams to perform risk assessments in a vacuum.

An integrated approach should incorporate the information and insights unique to each department, or business area, enabling a company to effectively manage risk enterprise-wide. For example, a physical security program that emphasizes access controls and surveillance systems can only help mitigate against theft and counterfeiting if the human resources and IT groups are also diligent in their efforts to prevent information breaches, including intentional sabotage. Also, the number of IT breaches from physical theft is almost impossible to track. Chain-of-custody security practices are most effective when counter measures are tailored to real threats. Applying threat intelligence and governance objectives to risk management helps to ensure that the right resources go to the right places.

This means that the perceived cost-of-compliance can be mitigated. Supply chain security programs share data-gathering and reporting requirements with other compliance areas, including but not limited to procurement practices, supplier-vetting and ongoing relationship management, chain of custody, human resources, business continuity, disaster response, Sarbanes Oxley, Occupational Health and Safety standards, information privacy protection, IT risk mitigation programs, documentation and processing, and physical security, and – of course – company policy. A silo approach both creates redundancies and reduces the benefits.

The good news for the second opportunity in supply chain security compliance is two-part. First, redundancies in the global compliance environment are driving innovation in integration and automation, raising the value of supply chain security for organizations that can effectively incorporate these programs into their overall governance strategy. Second, while physical supply chain threats remain real, the proliferation of cyber threats requires companies to connect physical and virtual networks that involve many of the same actors. Companies can make these connections using an integrated platform, enhancing the benefits, and reducing the cost of complying with individual initiatives.

APPROACHING SUPPLY CHAIN SECURITY THROUGH A GRC STRUCTURE

Threat mitigation tactics are typically standard business processes that can be shared across departments GRC a natural home for housing the risk management activities of different departments. Vendor risk management encompasses each relationship lifecycle, from the initial vetting process to establishing and implementing controls, audit, reporting protocols, and ensuring consistent, ongoing communication. Increasingly, these control checks are automated, which sets the stage again for a streamlined, less redundant approach to managing third-party security and compliance risk.

Both internal and government-sponsored supply chain security programs require a structured risk management approach, vendor surveying, action planning, documentation, and ongoing management. Meeting these objectives in the absence of process and information redundancies involves 1) streamlining information-gathering for multiple programs into one, if possible, annual survey and 2) correctly mapping the data so that reports can be tailored to one include multiple compliance programs. A GRC approach lowers the cost of compliance across the board by reducing reliance on an increasing number of niche reporting programs that, over time, will not scale and become costly to manage.

FROM A MODULO CUSTOMER CASE STUDY

"Where we previously performed assessments on 10% of off-site locations per year, integrating and automating third-party risk allowed us to assess all 300 plus sites. Using the Modulo Risk Manager Questionnaire mobile app streamlined site surveys on privacy and security requirements."

- Steve Bartolotta, GRC Program Manager at Yale New Haven Health Services

SUPPLY CHAIN SECURITY IS GOOD FOR BUSINESS

Enhanced targeting translates into benefits for businesses. An independent survey of the C-TPAT program conducted by the University of Virginia in 2010 identified the most concrete program benefits for businesses: workforce security improvements; decreased cargo release time by CBP; reduced time in CBP inspection lines; and increased predictability in the movement of goods. This means that both external and internal behavior changes are driving benefits, rendering supply chain security risk management good for compliance – and good for business.

Successful GRC programs leverage proven processes for compliance and risk management. These processes, such as ISO 31000 (see Figure 1) and others, adapt well to the five-step process laid out by US Customs Border Protection for C-TPAT compliance (see Figure 2). In fact, a cyclical interpenetration of what is often seen as a linear checklist can enhance the efficacy of C-TPAT compliance as well as ease the adoption of C-TPAT into the GRC program.

> **"Separating supply chain security management programs fuels the misperception that that these initiatives fail to address real threats."**

Companies using GRC as an integrated management platform will be a step ahead. Separating supply chain security management programs from each other as well as from other compliance initiatives requiring similar vendor risk management practices fuels the misperception that that these initiatives fail to address real threats.

This integrated approach is scalable and can be further streamlined through an automation platform. Software that cross-maps overlapping requirements and automates management and reporting enables users to dedicate a single platform for:

✓ Gathering and verifying vendor information
✓ Calculating risk scores
✓ Pooling risks
✓ Prioritizing and communicating corrective actions

Program managers can use the system's central database of vendor information to scale, implementing as many risk programs – and correlating profiles – as necessary.

Incorporation of C-TPAT can facilitate better Governance

Of all the potential intangible benefits, 'increases security awareness' and 'enhances security in supply chain' had the highest mean ratings (3.76 and 3.75 respectively on a 4 point scale). In each of these cases, roughly three quarters of all businesses considered them to be very important benefits. Other intangible benefits from the C-TPAT program included 'demonstrating corporate citizenship' and, 'improving risk management procedures and systems.'"

- US Customs-Trade Partnership Against Terrorism 2010 Partner Survey

Figure 1

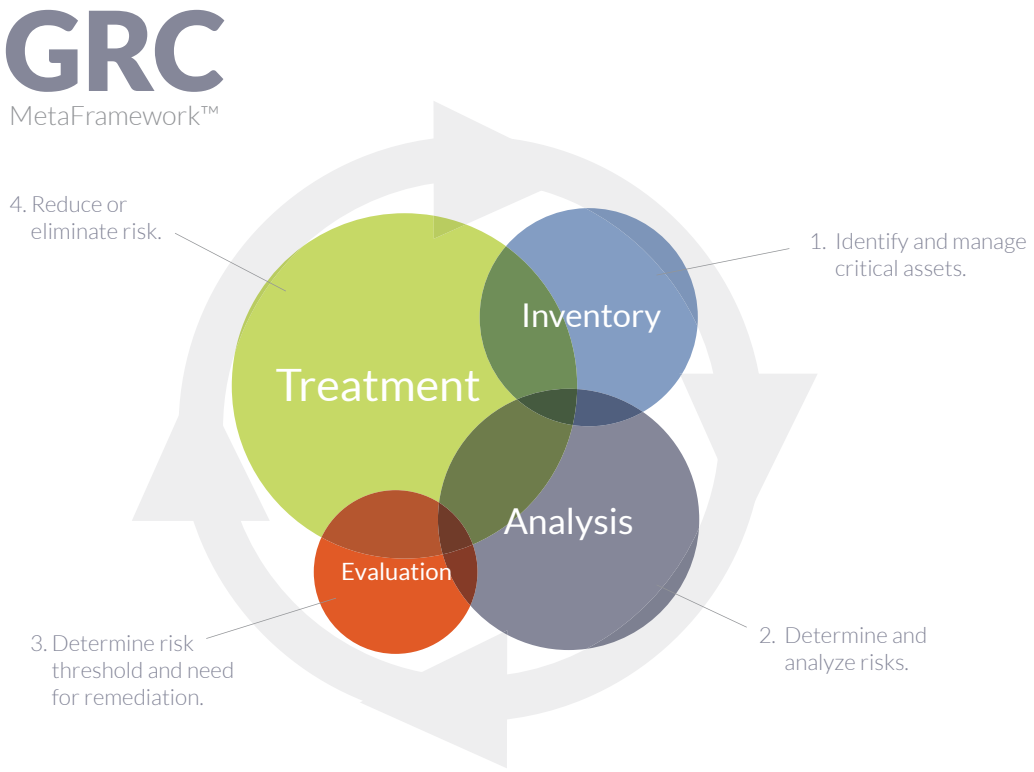
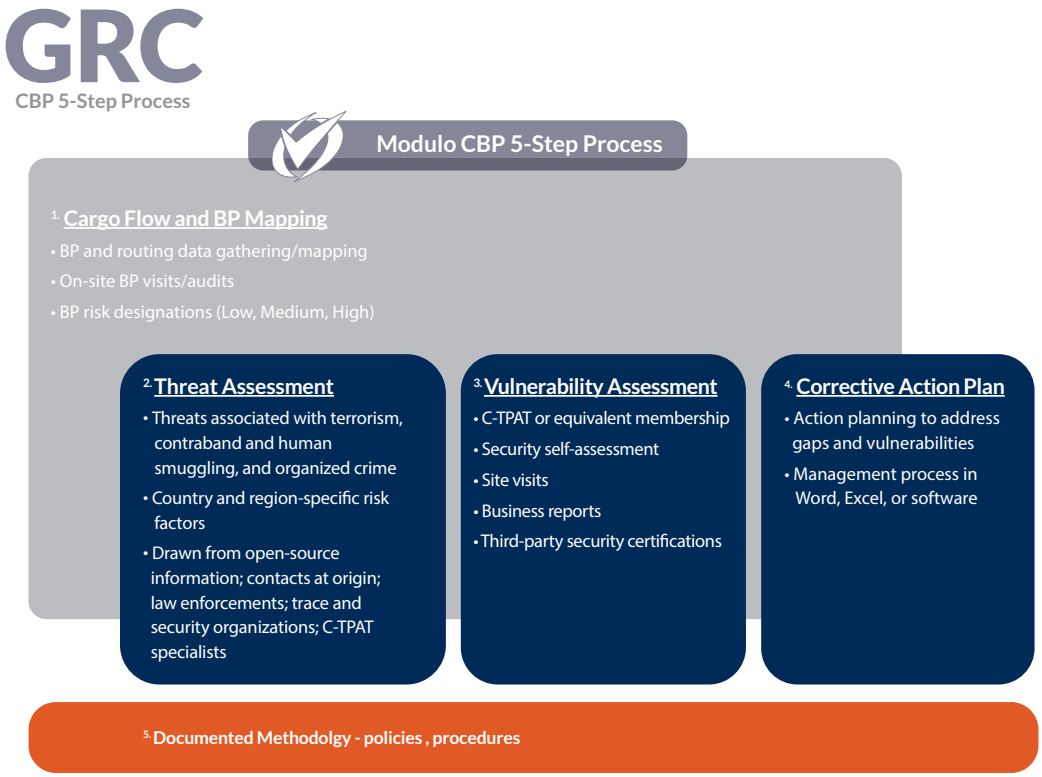


Figure 2



SUMMARY

Imagine a company with state-of-the-art cyber security risk management and monitoring tools failing to properly vet a service provider's network access. Hackers use the weak link in vendor point-of-sale access to install "Dump Memory Grabber" (e.g., BlackPOS), a new point-of-sale malware that copies payment data from thousands of customer records. The breach goes public; damage is compounded as the company gets widespread negative publicity; customers panic; the event instantly becomes a case study for "how not to..." In 2013, Target faced such a scenario.

The news is filled with stories of physical security matters impacting IT and vice versa. Yet global organizations need not be caught off-guard by scenarios such as the one Target faced in 2013.

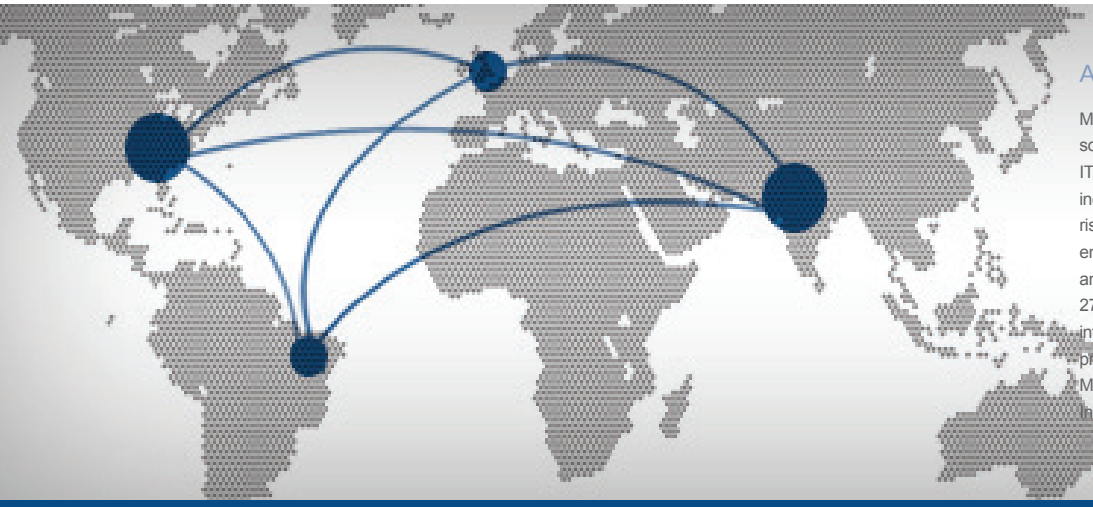
While security threats manifest differently in the physical and virtual spheres, organizations often find cooperation easier when managing major threats such as sabotage, espionage, and terrorism. Indeed, in high-risk scenarios, operating in a war-torn zone, sending executives to a dangerous country, shipping around the horn of Africa, security officers make little distinction in security management. This implies a perceived burden to managing risk in this way, yet automation software for integrated GRC is bringing cost down.

Identify opportunities to build governance around pre-existing business continuity or another proven process set of requirements. Programs fail when organizations plug automation in before establishing good processes. This is where a GRC program can help: by approaching supply chain security compliance from the perspective of company policy of "governance."

PORTIA MILLS is the Director of Marketing for Modulo. Ms. Mills has a background in technology start-ups, reputation risk management, and international economics and policy, having worked for BWise (now a NASDAQ OMX company), RepRisk AG, Serva Group, and ICx Harbinger Technologies. She holds a BA from Cornell University, an MA in International Relations and Economics from Johns Hopkins University and speaks French, Portuguese, Spanish, Haitian Creole, and other languages.

.

BARRETT HIGHTOWER has over 10 years experience in supply chain risk management, compliance, and trade policy research, analysis, and writing. Ms. Hightower has worked as a consultant with firms specializing in trade compliance and worked with public sector clients including US Customs and Border Protection and USAID. Her professional experience,
including work overseas, has resulted in an in-depth understanding of supply chain security policies, processes, and regulatory application.



ABOUT MODULO

Modulo is the leading global provider of GRC and Smart Government solutions. Over 1,000 customers globally leverage Modulo to monitor IT risk through automated workflow; report compliance against industry regulations, standards, and policies; prioritize operational risk through analytics and consistent business metrics; secure cloud environments; identify and remediate the most critical vulnerabilities; and much more. Modulo is the first company in the world to obtain ISO 27001 certification – the international standard for the governance of information security management systems – which guides Modulo's product development and proven risk reduction lifecycle methodology. Modulo continues to actively lead the creation and definition of international Standards in the GRC space.