National Institute of Standards and Technology
U.S. Department of Commerce

U.S. Resilience Project

BEST PRACTICES IN CYBER SUPPLY CHAIN RISK MANAGEMENT

NetApp
Anticipate, Mitigate, Improve

INTERVIEWS

Lee Wolfe
Senior Manager, Supply Chain

Wyman Stocks
Senior Manager, Global Information Security

Matthew Tardel
Director of Investigations and Security Programs

The Next New Things in Supply Chain Risk Management

- Cross-functional teams that address specific risks which cut across the enterprise, including information security and supply chain risks, in lieu of Chief Risk or Security Officers
- Quantitative decision-making tools to support investment and risk mitigation decisions
- Deeper supplier and component assessments by using a supplier "Yelp"-style rating system to create a pick-and-choose menu for business functions
- Robust monitoring of suppliers and component risks to enable faster decision making, and ultimately recovery

Company Overview

With more than $6 billion in revenue, NetApp creates innovative storage and data management solutions in the heart of Silicon Valley. Founded in 1993, the company has outlasted some of its initial customers, such as Tandem Computers. Over the past 20 years, it has become a global player in the market with 12,000 employees in more than 150 locations worldwide.[1] NetApp offers both products (Unified Storage, High Performance Sans Storage, Enterprise All-Flash Storage), as well as data sharing and storing services.

Culturally, NetApp embodies many of the values that signify successful high-tech companies, including adaptability, collaboration, teamwork and synergy.[2] These traits have been driving components behind key risk management initiatives at the company.

1 http://www.netapp.com/us/company/our-story/index.aspx

2 http://www.netapp.com/us/company/our-story/our-culture.aspx

Organizational Approach to Risk

NetApp has an Enterprise Risk Management Council (ERMC) responsible for corporate risk management. The ERMC has evolved and expanded over time and now includes members from critical functions such as finance, operations, compliance, HR, strategy and IT. The aim of the ERMC is to provide centralized risk strategy and governance, with decentralized execution.

For cross-cutting risks, like supply chain or information security, NetApp supports cross-functional teaming. On the supply chain side, the twin disasters of the Japan earthquake and Thailand floods in 2011 prompted the company to adopt a more structured approach to supply chain risk. Over the past three years, the SCRM team has expanded to now include supply chain security, supplier risk management and social environmental responsibility.

According to Lee Wolfe, Senior Manager for Supply Chain Risk Management, the company is exploring ways to facilitate collaboration among the different functions that touch supply chain risks. The management of risks is dispersed across the organization:

- IT group is responsible for cyber risks.
- Supply chain security deals with assessing and onboarding contractors, as well as counterfeit products.
- Supply chain risk management has principal responsibility for reviewing and rating suppliers and for the continuity of the supply chain.
- Product security, which is relatively new.

Bringing them together under an overarching security umbrella creates a more holistic approach to risk and risk mitigation.

In the same way, NetApp manages information security risks through a cross-functional team. Instead of a Chief Information Security Office (CISO) or Corporate Security Officer (CSO), NetApp has created an Enterprise Information Security Council (EISC) which is made up of leaders from various parts of the organization, including risk management, product security, IT security, physical security, supply chain and legal. The group meets at least once a month to discuss ongoing issues and concerns, plan and track IT security activities underway or in planning, and identify resources needed to push those activities forward.

Business Case for Supply Chain Risk Management

Because providing secure devices and services is a large part of NetApp's business — and many of their customers are government agencies — security is part of the company's DNA. Security is also coupled with quality to bolster the business case for investment.

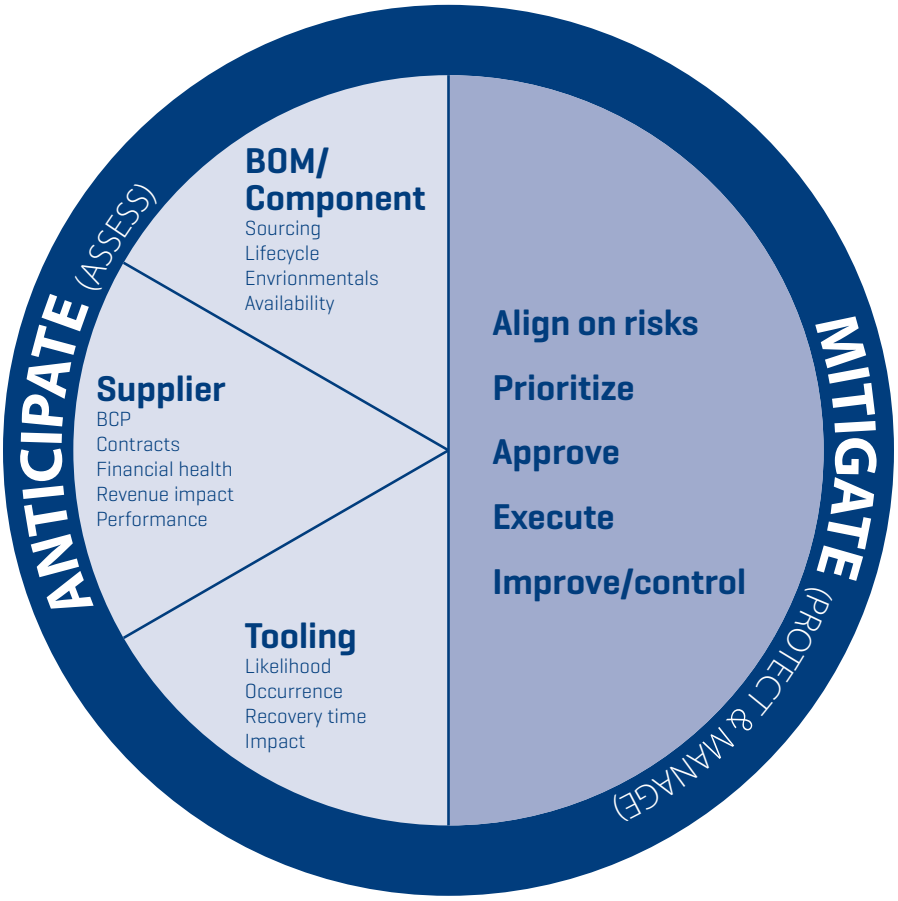
One problem for all companies is the lack of quantitative analysis to support investment in mitigation of risks that may never materialize. NetApp experts are beginning to develop analytic tools to aid its decision-making processes. First, a "crown jewel" initiative is seeking to identify the most valuable information in the company — the information that is core to the company's competitiveness. Second, the Information Security (IS) group is developing cost-benefit methodologies to aid risk management decisions. For example, one question is: At what point do cybersecurity alerts that distract workers' attention — such as an alert to staff about a possible phishing campaign — make financial sense? The group estimated how long it would take to read and react to the email (~30 seconds), and how many employees could be affected (all). Assuming a hypothetical cost of $4-5,000 per alert, the group can begin to calculate the breakpoint at which the potential cost of the cyber risk is greater than the cost of the cyber security measures.

Guiding Principles of SCRM: "Anticipate, Mitigate and Improve"

The philosophy of the supply chain risk management program is to optimize how the company anticipates, mitigates and improves supply chain risks. The risk management program scrutinizes risks to components, suppliers and tooling through each of these lenses.

The foundation of this approach is the ability to identify and assess risk. NetApp has developed a risk scoring methodology for both components and suppliers, built from its Bill of Materials (BOM). To do this, supply chain risk managers at NetApp developed a risk tool that creates component risk scores for the items on its BOM. The tool is based on information from industry tools, such as Silicon Expert, which provides engineering, life-cycle status, available inventory and environmental compliance data on 300 million electronic components — and NetApp's own supplier risk assessments. These include financial health, current performance, past performance and business continuity, and disaster recovery plan evaluations. What is created is essentially a "Yelp" review of suppliers. The business units have a "pick list" that they can review to assess the risks and opportunities of doing business with different suppliers.

Figure 1. NetApp Risk Assessment Framework



These ratings enable supply chain risk managers to pool information on suppliers and components into a consistent framework to evaluate risks. It also provides a way of influencing electronic manufacturing services (EMS) providers in their own selection of suppliers. Like many large manufacturers, NetApp keeps close tabs on its largest spend suppliers. However, that does not necessarily translate to tracking the highest risk suppliers. Institutionalizing risk scores on the BOMs as part of the EMS supplier rating allows NetApp to provide incentives for them to raise their score — and their market share — by picking lower risk alternatives among their supplier base. And the lower risk alternatives, both product and supplier, are identified by the tool.

One direct cost savings of the investment in tools to rate suppliers and components is that it has significantly reduced staffing needs to qualify alternative products in case of a disruption. A solution like this also enables design teams to look across other product lines' BOMs to leverage cost, usage and other data.

Managing Supplier Risk

Managing supplier risks is critical for NetApp, since its supply chain is 100 percent outsourced to third parties in the Americas, Europe/Middle East/African (EMEA), and Asia Pacific. The company maintains geographically diverse EMS partners to mitigate disruption risks and create redundancy at the manufacturing level.

There is ongoing monitoring of suppliers with "check and verify on a regular cadence." NetApp uses U.S.-based, certified professionals to inspect suppliers, verify that all requirements have been met and report back.

Supply Chain Continuity

Resiliency in the supply chain has become table stakes today, according to Lee Wolfe. "Too often, organizations wait until an industry-crippling event occurs to dig into the challenge of risk management." Noting that the Thai floods several years ago nearly crippled the storage industry — the floods drove a new focus at NetApp on robust risk management, as well as new policies to manage sole source risks.

In addition to the BOM and supplier scores, NetApp uses several third party providers (combined with its own team of analysts) to provide the SCRM team with alerts about pending and actual incidents that could affect the company's supply chain. This security operations center (SOC) monitors not only NetApp buildings around the world, but every supplier site. The SOC alerts enable quick reaction, but they do not create the capability to plan ahead for the "What If" contingencies. For that capability, NetApp mapped its supply chain and assessed time-to-recovery for each supplier site in case of disruption to identify the hot spots and areas in need of attention.

NetApp is also applying a geo-fencing capability for use in identifying continuity, physical or even cyber threats to the supply chain. A geo-fence is a methodology to define geographical boundaries. For continuity purposes, a geo-fence would trigger notifications in the event that disruptions — ranging from geopolitical unrest to weather to traffic disruptions — occurred within a defined area, such as a critical supplier location.

Cyber risks

NetApp addresses cyber-security from multiple approaches. First, Supply Chain Security is responsible for mitigating counterfeit materials. Physical Security has a robust process for onboarding vendors and contract software developers. This is done in partnership with IT and a relatively new Product Security group. The Product Security group was established in response to high profile attacks against Target and Home Depot, among others. All of these teams are part of the new EISC.

Three major areas of scrutiny include product security, supplier information security and network security.

Product security

Product security concerns are tempered by the fact that the IP that the company was built on — its crown jewels — was organically developed software. NetApp loads the software into products as they go to customers. Even their EMS partners do not have access to the proprietary code.

NetApp also leverages third party software, both proprietary and open. Similar to standard industry practice, there is no single strategy for assuring the integrity of purchased software. For proprietary code, visibility depends on the types of warranties and indemnification that the supplier is willing to offer, and that determines how much visibility the company needs into the software provenance. In some cases, NetApp may choose to license binaries only. In others, it will require the source code.

For open source, the software code is available, so it can be scanned and inspected. However, in the wake of the Heart Bleed vulnerability in 2014, NetApp became a founding member of a coalition jumpstarted by the Linus Foundation. The Core Infrastructure Initiative now includes 20 organizations that contribute roughly $6 million toward addressing open-source software projects that are critical to the functioning of the Internet and other major information systems.

From a hardware perspective, the cyber risks are also scrutinized carefully. Because many of NetApp's EMS partners also do business with U.S. agencies, including the Department of Defense, they have very strong security policies and capabilities. Those capabilities are verified by NetApp security teams on a regular basis.

Supplier information security

The Information Security group has the lead on supplier assessments. NetApp does not automatically assume its suppliers will do the right thing. However, unlike some companies — which deploy 30-page spreadsheets broken down into different worksheets that are in turn broken down into different aspects of information security — NetApp uses a five-page questionnaire that examines supplier processes and protocols for managing and protecting data. This includes information about how suppliers manage and protect NetApp's data, including:

- How they manage NetApp data;
- How they store NetApp data;
- How the date is encrypted;
- How long the data is retained; and
- How the data is destroyed when the partnership is dissolved.

Wyman Stocks, Manager of Global Information Security noted: "Our goal is discovery rather than an excess of hard and fast requirements."

Network Security and Third Party Interfaces

On occasion, third parties may need to connect to the NetApp network to transmit data — for example, shipping information or manufacturing orders. NetApp controls those connections very tightly. For the vast majority of suppliers, NetApp positions networking gear at their sites and controls its use. Only a few machines at a given vendor are allowed to connect, and NetApp manages the network address translation. Access is controlled on both ends. The VPN "tunnel" is restricted to just a few machines, which have only limited — and tightly controlled — access to the NetApp network

Physical and Transportation Security

NetApp recently received U.S. government Customs-Trade Partnership Against Terrorism (CTPAT) certification — a process that help build bridges and stronger lines of communication between supply chain risk management, security and NetApp's suppliers. The certification process itself resulted in more collaboration with NetApp's suppliers, more visibility into shipments, and more granular scrutiny of the physical security standards at supplier locations. In some cases, this involved a full site security audit by the border patrol as part of the verification process.

According to Director of Investigations and Security Programs Matthew Tardel, the onsite scrutiny of security processes looks at small details, including:

- What kind of access controls are in place?
- How many digital cameras are onsite? What make, model and resolution? How many days of activity are stored?
- What is the inventory in-take process?
- Where is equipment physically stored? Who has access?

The level of physical security required and frequency of audits is influenced by the criticality of the supplier, and the value and volume of business.

As important, the security team is focused on building trusted relationships with their counterparts at supplier companies. That creates both a source of information and insight on how problems might have occurred, and a source of learning on practices or protocols by individual suppliers that could be extended to others in the network. For example, one supplier required employees not only to pass through a magnetometer at the end of the day, but also turn their electronic devices on or off (after having found that plant employees were stealing chips through the hollowed-out shells of their phones and devices).

Standards: Compliance with ISO 9001, ISO 14001, ISO27001

NetApp has been a member of the EICC since 2013 and expects its suppliers to comply with both the EICC Code of Conduct as well as its own Supplier Code of Conduct.[3] NetApp complies with the Dodd-Frank requirements regarding sourcing conflict minerals only from socially responsible suppliers in the Democratic Republic of Congo.[4]

According to Lee Wolfe:

> "NetApp has significant market share of storage operating system worldwide. It's extremely important for us to make sure that our products and systems are secure. Our reputation depends on the ability to secure our products and systems. It's all a matter of strong standards and using trusted third parties as a redundant check to ensure robustness."

3 http://www.netapp.com/us/company/our-story/conflict-minerals.aspx

4 http://www.netapp.com/us/system/pdf-reader.aspx?cc=us&m=Conflict%20Minerals%20Policy.pdf&pdfUri=tcm:10-120521