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

U.S. Resilience Project

BEST PRACTICES IN CYBER SUPPLY CHAIN RISK MANAGEMENT

Fujitsu Network Communications
Managing Supply Chain Risks in Optical and Wireless Networking

INTERVIEWS

Barrie Hall
Senior Vice President–Fulfillment, Fujitsu Network Communications

Jonathon Steenland
Head of Strategic Security, Fujitsu Network Communications

Stephen Pichocki
Senior Sales Manager, Service Solutions, Fujitsu Network Communications

Alan Dorr
Senior Director of Purchasing, Fujitsu Network Communications

The Next New Things in Risk Management

- FNC's Enterprise Security Intelligence program (ESI) will transition cybsersecurity from perimeter and point defenses to analysis of network, systems and other operational data to detect anomalous activity.
- Information Security contractual requirements followed up with hands-on management of supplier IT, with 100 percent of IT personnel and equipment managed by FNC.
- First tier suppliers are required to dual source critical components from the sub-tiers.

Company Overview

Fujitsu Network Communications (FNC) is a subsidiary of Fujitsu, the world's third largest provider of IT services.[1] FNC designs, manufactures and maintains a variety of network equipment and combines wireless, wireless and software technology with multivendor services expertise to deliver end-to-end network integration and management solutions. FNC is a top U.S. patent-holder in optical networking technology and the only major optical networking vendor to manufacture its own equipment in North America. Based in Dallas, Texas, the company's principal customers are the telecom and cable industries, but it also serves research, financial services and utility markets as well as federal, state and local government agencies.

1 http://www.servicestop100.org/it-services-companies-top-100-of-2010.php.

Organizational Approach to Supply Chain Risk

Supply chain issues fall under the purview of the Senior Vice President for Fulfillment, Barrie Hall. Supply chain risk management (SCRM) directly involves procurement, quality assurance and component engineering organizations. Two of these groups report directly to the SVP Fulfillment, and the third is in the same building — an organizational structure that enables risk collaboration and communication.

Business Case for Supply Chain Risk Management: SCRM is an essential business function. According to Barrie Hall:

> "Trying to do an ROI on the unknown is virtually impossible. Experience has taught us that there are real risks to the supply chain. When you recognize how those risks could impact your business, that alone is sufficient to garner the support for risk management that we have in place today."

Guiding Principles of Supply Chain Risk Management

FNC has identified its two biggest supply chain risks as:

1. Regional catastrophic event, and
2. Vendor financial instability.

Regional catastrophic events: The Japanese tsunami and Thai floods in 2011 had a profound impact on a wide range of industry sectors because of the concentrations of high technology manufacturing in these areas. One of FNC's primary risk mitigations strategies was to dual source as many products as possible. Because some parts cannot be multi-sourced, FNC has gone back to its suppliers to ask whether their components are multi-fabbed in different regions. From a risk perspective, multiple fabs in different geographies provides almost as strong a mitigation strategy as dual-sourcing.

Vendor financial stability: Financial stability is the other key vendor risk priority. FNC scrutinizes financial performance indicators — for both public companies and privately owned — on an annual basis.

Supply Chain Risk Management

Vendor Management: SCRM begins with the vendor qualification process. Vendors are qualified on several levels. The procurement group assesses vendor viability from a financial standpoint, while the quality group provides an assessment on quality control system processes and systems. A level below that, component and design engineering teams work with the quality group to assure that the individual products from the vendor meet the companies' specifications. Site assessments for new suppliers are common, with quality and security a key focus of the site assessment.

Before onboarding, vendors fill out an in-depth questionnaire annually. However, the core supply chain risk management groups — procurement, quality and component engineering — meet monthly to assess supply performance, problem areas and actions to improve the robustness of the supply chain. When a vendor falls into the "high risk" category, they are then reviewed monthly instead of annually until their problems are resolved. If a vendor does not move out of the "high risk" category quickly then, based on their level of stability and product quality, their status may trigger a site visit or reduction in market share. Whenever a site visit team is dispatched to visit those vendors, the results are debriefed to the cross-functional team.

In addition to the internal reviews described above, FNC also conducts quarterly key Supplier Performance Reviews (SPR). During these SPR meetings, FNC purchasing and quality review supplier performance in face to face meetings with each supplier. These discussions include review of Business Continuity Plans.

FNC has also raised the bar on their vendors and supplier contractually. The contracts now include a range of requirements from Business Continuity Plan (BCP) submissions to indemnification, product notifications and physical security.

Supply Chain Continuity: FNC maps its tier 1 suppliers to identify critical chokepoints and single source points of failure. The supply chain is sufficiently large that tier 1 suppliers are required to manage risks at the sub-tier level, including a requirement for dual sourcing of critical components.

Quality and Integrity Compliance: FNC follows a structured New Product Introduction (NPI) process for hardware products. They perform numerous product performance validation test throughout the NPI process. Before releasing a product for General Availability (GA) to customers, there is additional qualification testing at the manufacturing and assembly level to verify the performance of the product in extreme conditions. Once FNC engineering is confident that they have a robust product to deliver to the field, the product goes GA, subject to sample inspections on a scheduled basis.

As long as the components pass sample inspections, they are only subject to regular, routine re-inspections. If a component fails the spot check, however, FNC will institute a temporary 100 percent inspection of incoming components, until such time that the vendor demonstrates that it has fixed the problem

On the software side, there is a similar process. Software verification tests at the end of the software development cycle assures that the software is performing as expected. If potential weak points are identified, the company generates a Problem Tracking Record (PTR). If the software is deemed releasable, the PTR log is maintained and the problem addressed on the next release.

Managing Cyber Security Risks: FNC has a dedicated in-house cyber security office that reports to the CIO. According to Jonathon Steenland, Head of Strategic Security at Fujitsu, this office has two roles:

1. An operational role to manage all activities related to cyber security and IT networking at FNC; and
2. A broader advisory roles throughout the Fujitsu organization to help implement cyber programs.

FNC's security team helps establish policy, procedures and technology solutions across Fujitsu's 500 companies, which are localized to different regions. The FNC campus, which combines manufacturing, research and development, full software automation, and services in one subsidiary provides an ideal testing ground. When a security solutions works for the FNC subsidiary, it tends to scale well to the rest of the company.

Enterprise Security Intelligence: From FNC's perspective, "the threat landscape has evolved from automated indiscriminate attacks against computers via worms and viruses to highly targeted-attacks against individuals and data via human-led teams dedicated to the task of stealing competitive and strategic intelligence in the possession of the victim. In many cases, the attacks are dedicated to the acquisition of a particular set of data, whether it be engineering diagrams, source code, merger plans, non-public financial statements or other information considered to be of strategic, competitive or financial benefit to the attacker or its sponsors."[2]

Automated attacks that do not employ human discretion in target acquisition of exploitation are easily detected and stopped by traditional controls: perimeter firewall controls, intrusion detection systems, anti-viruses. More recent attacks against large companies, however, have targeted proprietary information, either stored on or accessed by end-user devices and servers. These attacks are tailored to exploit known weaknesses and tuned to evade detection:

> "An organization's ability to detect and respond effectively to these new threats is directly linked to its ability to capture and analyze networks, systems and other operations data for anomalous activity and to collaborate with other organizations to share lessons learned and situational awareness information."[3]

According to Jonathan Steenland:

> "It is no longer sufficient to rely solely on perimeter and endpoint device protection to ensure the confidentiality, integrity and availability of company-critical IT assets. Instead, a comprehensive security plan must include advanced analysis of data not traditionally associated with information security: in particular, log and other data related to IT operations, personnel and physical access can be leveraged to provide a holistic view of anomalous and potentially malicious activity on sensitive networks."[4]

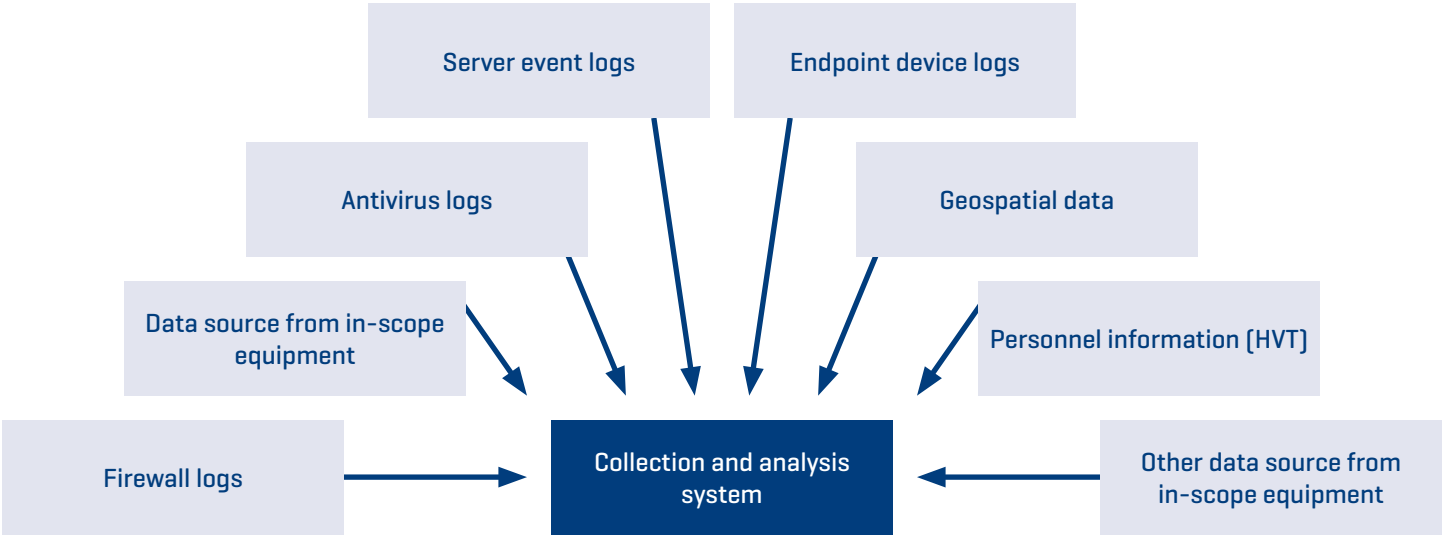
Figure 1 illustrates the kinds of data that can be used to detect more advanced attacks.

2 Enterprise Security Intelligence: A Cornerstone of Innovation, Jonathan Steenland, Fujitsu

3 Ibid

4 Ibid

Figure 1: High-level ESI Process



At the heart of this analytic capability is the Advanced Security Innovation Center (ASIC), a state-of-the-art analysis center that has leading technology — Fujitsu developed, commercial off the shelf, and custom — to provide ESI analysts with the tools they need to perform their work. The goal is to detect, deter and disrupt adversarial attacks across the Fujitsu network of companies. The ASIC also creates an incubator for security personnel and solutions. Figure 2 captures the key missions of the ASIC.

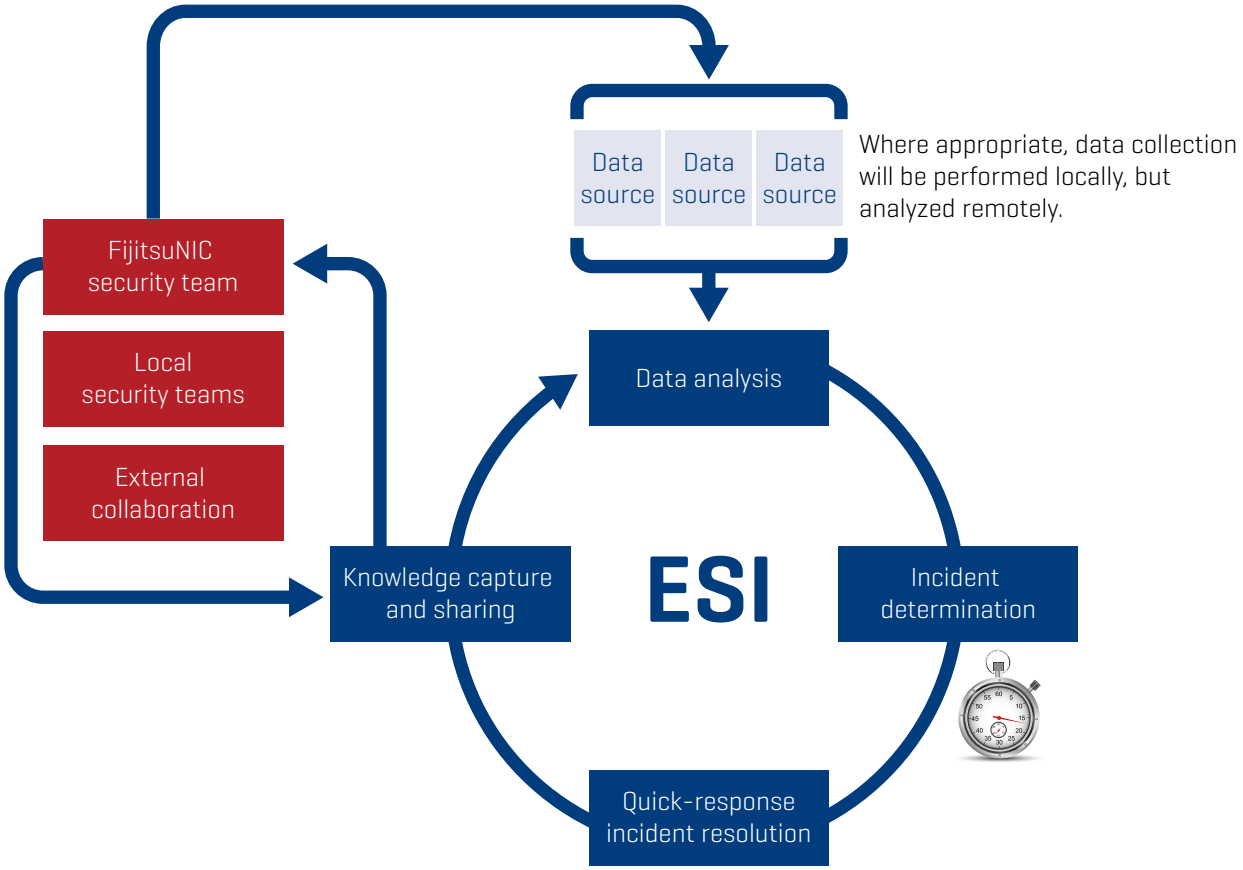
Figure 2: Advanced Security Innovation Center (ASIC)

PROGRAMS	**People**	**Processes**	**Technology**
	Top gun training	Enterprise security intelligence	Security product testing
DELIVERABLES	Trained personnel	Advanced analytics	Case studies
	Formalized Security training	Intelligence reports	Product evaluations
	Red team / Blue team	Monthly newsletters	Product vulnerability testing
	SME relationships	Standard operating procedures	Product certifications

If the data analysis indicates that a compromise has occurred, ESI maintains e a "quick response" capability to eliminate the emergent threat through near real-time remediation. A third objective is to enhance the value of information gathered and analyzed through a series of strategic information-sharing partnerships. The ESI will establish formal strategic collaboration arrangements with Fujitsu research and development groups; government and law enforcement; universities and industry groups as well as other leaders in the security intelligence space.

Figure 3 provides a high level look at the ESI process.

Figure 3: Enterprise Security Intelligence



Supply Chain Cyber Security

Vendor access to FNC's network is strictly controlled. All vendors and contractors are entered into FNC's SAP system. The system authenticates identify and other key factors (e.g., that legal non-disclosure agreements or that export compliance checks have been conducted). Only when these checks are complete can vendors and contractors be provisioned with limited accounts. There are a couple of different levels of security.

- **Secure Remote Development Extranet:** Fujitsu maintains a Secure Remote Development Extranet for partner communications and data-sharing. The data, for example, access to hardware design schematics, is maintained in FNC data centers. With this security approach, FNC can maintain control over who's connecting into the system, what data can be accessed, what data is leaving the system
- **Global Information Security Controls:** One specific tool across the Fujitsu companies and their suppliers is the Global Information Security Controls (GSIC). Closely modeled on the ISO 27001 standard, the framework provides a base line for IT risk assessment and management. Depending on the level of supplier access into FNC networks, this framework may be built into supplier's contractual obligations. For partners that require a great deal of access to the FNC environment, the security control language may simply be cut and pasted into the contract.

  Going an additional step further, for critical partners, FNC follows up with hands-on IT management in those locations. In certain areas with bigger clients, FNC takes a proactive approach to cyber risk management. According to Jonathon Steenland: "If it's an offshore environment, we treat it as branch office — no different from what we would do in the States. All the equipment and personnel in those environments are 100% dedicated to FNC. We consider it a remote office with our folks providing the IT support."

Additional Contract Requirements

FNC contractually obligates their suppliers to be TL9000 certified. Established in 1988, TL9000 is the telecommunications industry specific version of ISO9000 for quality management systems.[5] In its latest revision, TL9000 now has provisions related to physical, network and product security including:

> 7.1.C.3 Product Security: The organization shall establish and maintain methods for the identification and analysis of security risks and vulnerabilities for the product throughout its life cycle. The results of the risk analysis shall be sued to support secure network operation by prevention or mitigation of security vulnerabilities in the product design and operational controls. The continuing effectiveness of the design and operational controls shall be assessed throughout the product life cycle by the selection and use of appropriate security measurements.[6]

Several notes to this provision require attention to risks related to possible exploitation of vulnerabilities through communication and/or use/operator interfaces of the product. It defines operational control as a means of managing risk, including policies, procedures, guidelines, practices or organizational structures which can be administrative, technical, management or legal in nature. Examples of operational controls include a process for granting and removing access (both physical and logical) to systems, documented operating procedures, change control procedures and procedures to control the installation of software on operational sysems. TL900 references a Security Measures Guidance document which can be used as a resource in selecting and establishing appropriate security measures for the product.

Security Awareness: FNC's physical security team manages visitor access through stringent policies and annual employee training. The company organizes "Spot the Bogey" contests with give-IPOD give-aways to raise awareness of security risks. Jonathon Steenland calls it the best $100 invested in security.

5 http://www.tl9000.org/about/tl9000/overview.html

6 http://www.tl9000.org/handbooks/documents/TL_9000_Requirements_Handbook_Release_5.5_Changes.pdf

Gaps

FNC sees two gaps that NIST might examine in the next iteration of the cyber framework.

Product Vulnerability Testing: FNC is increasing its own product vulnerability and security testing, but would like to see more widespread adoption of such practices in their industry. This is in response to increased number of requests and proactively preparing for potential federal legislation in the US that would require companies in industries such as critical infrastructure and defense to identify the Bill of Material (BOM) for source code in products and validate them against known vulnerabilities.

Cyber Insurance: Cyber insurance offers a path to get standards in place to incentivize investments in cyber security. There is a perhaps apocryphal story told about a farmer in a small town who invented sprinkler systems for fire prevention. To create a market for his new product, he set his barn on fire and activated the sprinkler system to put the fire out. But, the market didn't budge until 20 years later when regulators and insurance companies made it a requirement for buildings to install sprinkler systems. The hope is that cyber insurance will have the same impact.