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

U.S. Resilience Project

BEST PRACTICES IN CYBER SUPPLY CHAIN RISK MANAGEMENT

Boeing and Exostar
Cyber Security Supply Chain Risk Management

INTERVIEWS

Robert Shaw
Computing Security & Information Protection Specialist, Boeing Information Security

Vijay Takanti
Vice President of Security and Collaboration Solutions, Exostar LLC

Tim Zullo
Marketing Director, Exostar LLC

The Next New Thing in Cyber Security Supply Chain Risk Management

- Collaborative community auditing capabilities for real-time, continuous cyber supply chain risk assessment, identification and management

Company Overview

Boeing is the world's largest aerospace company, as well as a manufacturer of commercial and defense airplanes, space and security systems. At this time, the company is organized into two business units: Boeing Commercial Airplanes and Boeing Defense, Space & Security, both supported by Boeing International. It is based in Chicago, Illinois, with more than 160,000 employees throughout the United States and 65 other countries.[1] Boeing prides itself on being an innovation powerhouse in both its products and processes.

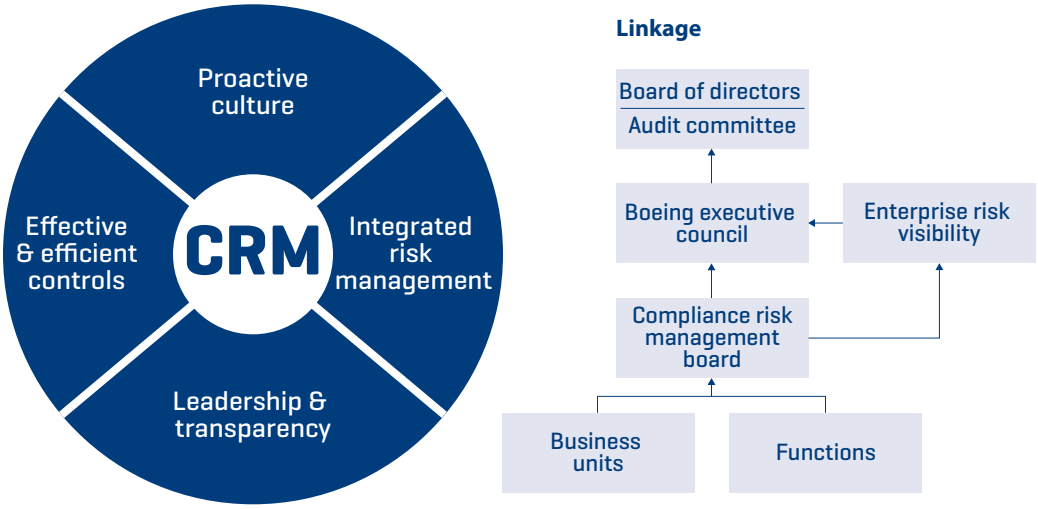
As befitting of a global manufacturer, its supply chain is enormous in its size, geographic distribution and number of tiers. The commercial division has more than 5,400 first and sub-tier suppliers.[2] The famous 787 "Dreamliner" alone has 2.3 million parts to it, and most of those come from the extensive global supply chain.

1 http://www.boeing.com/company/key-orgs/boeing-international/index.page

2 http://www.boeingblogs.com/randy/archives/2013/02/supply_chain.html.

Organizational Approach to Cyber Security Supply Chain Risk Management

Given the size and complexity of the Boeing company, there are numerous organizations and teams that have a hand in the corporate supply chain risk management effort. Within Boeing's Shared Services Group are teams dedicated to Security and Fire Protection and Supplier Management, which procures non-production goods and services.[3] Compliance is a huge focus for the company as illustrated by its approach to Compliance Risk Management.[4]



- Embedded in businesses and functions
- Driving integration
- Leadership engagement

For cyber security specifically, numerous organizations are also involved, ranging from Information Security and Cyber Security teams to Procurement. To be effective, these teams need to communicate, coordinate and collaborate on a regular basis. The Information Security (IS) organization takes the lead for managing vendor IT security as it relates to accessing Boeing's network and/or data assets, and works with Procurement to ensure all IS access requirements are met by suppliers during the on-boarding phase.

3 http://www.boeing.com/company/key-orgs/ssg.page.

4 http://www.boeing.com/resources/boeingdotcom/principles/ethics_and_compliance/pdf/crmb_charter.pdf.

In the procurement context, IS covers three scenarios:

1. Vendors who need access to Boeing's network
2. Vendors who need access to data assets on the network
3. Vendors who need access to data assets that are not on the network

Cyber Security Requirements in Contracts

For Boeing's IS team, cyber security supply chain risk management begins with the contract negotiations process. The Procurement group is responsible for the entire vendor management and selection process, but it defers to IS regarding vendor cyber security requirements and compliance. To this extent, IS has developed contract language that covers requirements and expectations of the supplier base for each of the three IT procurement scenarios. These suppliers are typically installing or maintaining Boeing's software and infrastructure. Nonetheless, other organizations throughout Boeing also leverage the contractual language developed by the IS team to manage, for example, cyber risks in software embedded in purchased components or control systems.

The IS team gets involved early in the procurement process to ensure that internal stakeholders fully understand the security requirements that vendors are expected to follow. If a vendor pushes back on the contract requirements, the IS team is brought directly into the negotiation process so both parties can understand each other's goals and positions.

Cyber Security Standards: The IS team determined that, rather than develop homegrown security requirements, Boeing's requirements would leverage existing standards. The primary standard is the Critical Security Controls (the Controls), a recommended set of actions for cyber defenses developed by the Council on Cyber Security that provide ways to thwart the most pervasive attacks.[5] Boeing also looks to other standards — FedRAMP,[6] ISO27001, SOC 2 Type II, CSA STAR 2,[7] and their own internal questionnaire based on the Controls.

Flow-Down of Cyber Security Requirements: Boeing expects its suppliers to flow down these security requirements to sub-tier suppliers. This includes Boeing's IT service providers, e.g., companies that provide infrastructure support, application support, and IT maintenance where the work, in many cases, has been off-shored.

5 http://www.counciloncybersecurity.org/critical-controls/.

6 http://www.gsa.gov/portal/category/102371.

7 https://cloudsecurityalliance.org/star/.

Sub-tier suppliers, no matter the location, are expected to meet the same cyber security requirements as first tier suppliers. The precise level of security required depends on the service or product being provided.

Cyber Security Assurance: Boeing relies on Exostar to continuously monitor, measure and mitigate cyber security risk throughout its multi-tier supply chain. Exostar was formed in 2000 as a joint venture between five of the world's largest Aerospace & Defense companies — Boeing, BAE Systems, Lockheed Martin, Raytheon and Rolls Royce. Although Exostar began as a supply chain portal to bring buyers and sellers together in the aerospace industry, it has evolved into a cloud-based, online platform to ensure secure connections across the global aerospace and defense supply chain ecosystem.

The transformation began in 2007 when the aerospace companies were called in to discuss an emerging concern at the Department of Defense: Leaks of critical company and product data through the supply chain, which was a lose-lose situation for both sides. On the industry side, the loss of intellectual property affected both jobs and the companies' bottom line. On the DoD side, that loss of proprietary information had the potential to affect the nation's military posture.

The aerospace companies, later joined by Northrup, took the lead to jointly develop and deploy a number of tools to manage the information-sharing process more securely and to protect information throughout the supply chain ecosystem. One set of tools was designed to secure industry supplier portals by strengthening access controls and identity management systems. Exostar's Federated Identity and Access Management solution, known as the Managed Access Gateway (MAG), allows more than 100,000 organizations to securely and seamlessly share information across partner networks, thus creating a "do it once — share to many" model.

A second tool, the Partner Information Manager (PIM), was developed by an industry working group over an 18 month period to ensure that suppliers were capable of protecting critical information assets and network connections. The PIM establishes common cyber security definitions and standards for aerospace industry suppliers — setting minimum thresholds of compliance for every supplier. PIM's value extends beyond the buy-side to the supply-side. Partners working with multiple organizations need only complete a questionnaire once, thus easing the administrative burden, eliminating redundancy and inconsistency, and delivering the information that leads to improvements in their overall vulnerability.

According to Vijay Takanti, Vice President of Security and Collaboration Solutions:

> "By offering connect-once, single sign-on access, Exostar strengthens security, reduces expenditures and raises productivity so customers can better meet contractual, regulatory and time-to-market objectives."

Exostar's PIM application platform and data, with controlled access via MAG, helps its members overcome traditional supply chain risk management challenges such as:

- Limited visibility into partner/supplier risk
- Limited ability to share information from one supplier to multiple buyers
- Limited industry standard measurements to assess and address risk
- Limited standard platforms providing an easy-to-digest, correlated dashboard overview of partner/supplier risk
- Long lead times to evaluate partner/supplier relationships
- Redundant processes to collect partner/supplier risk data
- Limited roadmaps to improve supplier vulnerabilities
- Limited tools to measure improvement in real-time and over time

Supplier data is continuously collected and evaluated by the Exostar's PIM analytics engine, thus allowing organizations to better measure and mitigate risk as it relates to the work being performed. With this model, new partners can be on-boarded and existing partners can be reassessed more confidently and rapidly — ensuring suppliers meet the necessary levels of assurance as statements of work, standards and business operations evolve. Importantly, because the threat environment is constantly evolving, the tool can be readily adapted to incorporate any new standards that may emerge.

Cyber security Questionnaire: Exostar's online questionnaire for cyber security is structured around 22 "Control Families." Within each of the Control Families, Exostar drills into more specific "Control Activities" and ascertains if a control has — or has not — been fully implemented. Exostar calculates a capability level for each Control Family and, where vulnerabilities or deficiencies are found, recommends a set of remediation activities to help the vendor mitigate risks and comply with the requirements set forth by Boeing and other buyers.

Table 1 depicts the maturity levels defined by the Exostar system — individual controls are rated from 1 to 5. Basic controls score in the 1-3 range. More advanced controls would score in the 4-5 range. Based on the survey responses, Exostar's PIM derives a capability score for each supplier, which is used to assess cyber risk in the supply chain.

Table 1: Exostar's Cyber Security Maturity Levels

Level	Definition
0	Indicates no or minimal cyber risk management program; significant cyber protections are lacking; additional risk mitigation must be implemented.
1	Indicates a basic level cyber risk management program; some protections in place, but additional risk mitigations must be implemented.
2	Indicates a moderate level cyber risk management program; good protections in place, but additional risk mitigations are required to protect sensitive information.
3	Indicates a solid performing cyber risk management program; strong protections have been implemented; advanced threats are understood and steps have been taken to address with specific controls; additional risk mitigations are likely needed to protect against advanced attacks.
4	Indicates a cyber risk management program that can detect, protect against, and respond to advanced threats; specific advanced controls are implemented.
5	Indicates a cyber risk management program that can detect, protect against, and respond to advanced threats; specific advanced controls are implemented and optimized on an ongoing basis.

Table 2 identifies: 1. The 22 Control Families covered by the Exostar questionnaire; 2. Objectives of the controls; and 3. Examples of specific controls required to demonstrate different levels of cybersecurity maturity.

Table 2: Categories Examined in On-line Audit of Supplier Cybersecurity Controls

Control Families	Objective	Examples
1. **Inventory of Authorized and Unauthorized Devices**	The control objective is to manage all hardware devices on the network so that only authorized devices are given access and unauthorized or unmanaged devices are found and prevented from gaining access.	Basic controls include: an asset inventory of systems or devices that connect to public or private networks; information about every device (its network address, purpose, asset owner, and department). More advanced suppliers will have a capability for automatic inventory updates, network level authentication capabilities, ability to isolate systems or devices in the event of attack, and requirements for client certificates to validate and authenticate systems prior to connecting.
2. **Inventory of Authorized and Unauthorized Software**	The control objective is to manage all software on the network so that only authorized software is installed and can execute and that unauthorized and unmanaged software is found and prevented from installation or execution.	Basic controls include: capability to block dangerous file types; development of a list of authorized software and version, and deployment of software tools to identify and record the types of software installed, its version number and patch level. More sophisticated controls include: "whitelisting" applications that only permit software included on the whitelist; software with signed ID tags; integration of software and hardware inventories; regular scanning for unauthorized software; and virtual and/or air gapped systems to isolate high-value or higher risk applications.
3. **Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers**	The control objective is to establish, implement and activity manage the security configuration of laptops, servers and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.	Basic controls include: automated patch management, limited administrative privileges, and hardening of operating systems (e.g. removal of unnecessary accounts or services, closing open or unused network ports, intrusion detection systems etc.). More sophisticated suppliers will have strict configuration management, file integrity checking tools, automated configuration monitoring systems,
4. **Continuous Vulnerability Assessment and Remediation**	The control objective is to continuously acquire, assess and take action on new information in order to identify and remediate vulnerabilities and minimize the window of opportunity for attackers.	Basic controls include automated patch management tools and software, vulnerability scanning tools run on a weekly or more frequent basis, and comparisons of back-to-back vulnerability scans. More sophisticated controls include log monitoring associated with scanning activity to ensure legitimacy; risk rating of vulnerabilities, subscription to vulnerability intelligence services; measurement of pathing delays; evaluation of critical patches in test environment.

Control Families	Objective	Examples
5. **Malware Defenses**	The control objective is to control the installation, spread and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering and corrective action.	Basic controls include automated tools to continuously monitor workstations, servers and mobile devices with anti-virus, anti-spyware personal firewalls and host-based IPS functionality; cloud-based anti-malware software; configurations that will not auto-run content from removable media; automatic scans of removable media when inserted; capabilities to scan and block email malicious code or suspect files types attachments at the organization's gateway. More sophisticated controls include behavior-based anomaly detection; domain-name system query logging for known malicious domains; limited use of external devices to those with business need; or network-based anti-malware tools to identify executables in all network traffic.
6. **Application Software Security — In-house Developed Software and - Purchased Software**	The control objective is to manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect and correct security weaknesses.	For in- house developed software, there are a range of basic controls: explicit error checking for all input, testing for coding errors or potential vulnerabilities prior to deployment; training in secure coding for all software development personnel, and separate environments for production and nonproduction systems. For both in-house and purchased software, basic controls include testing for common security weakness with automated web application scanners prior to deployment and standard hardening configuring templates for applications that rely on a database. More advanced controls for application software, in-house or purchased include: deployment of web application firewalls that inspect all traffic flowing to the web application and scrutiny of the product security process of the vendor (history of vulnerabilities, customer notification, patching/remediation).
7. **Wireless Access Controls**	The control objective is to secure the wireless local area networks, access points and wireless client systems.	Basic controls include assuring an appropriate level of encryption; disabling peer-to-peer network capabilities and wireless peripheral device access, unless such functionality meets a documented business; and configuring network vulnerability scanning tools to detect wireless access points connected to the wired network. More advanced controls include: ensuring that wireless networks use authentication protocols; disabling wireless access in hardware configuration, where no documented business need exists; ensuring that each wireless device connected to the network matches an authorized configuration and security profile; and using wireless intrusion detection systems to identify rogue devices and detect attack attempts or compromises.

Control Families	Objective	Examples
8. **Data Recovery Capability**	The control objective is to ensure the adequacy of processes and tools to back up information with a proven methodology for timely recovery.	Basic controls include: ensuring that stored backups are properly protected and encrypted and that each system is automatically backed up at least once a week. More advanced controls include: regular testing of data on backup systems by performing data restoration processes and ensuring that key systems have at least one backup destination that is not continuously addressable.
9. **Security Skills Assessment & Appropriate Training**	The control objective is to identify the specific knowledge, skills and abilities needed to support defense of the enterprise and develop and execute an integrated plan to assess and identify skills or training gaps.	Basic capabilities include: perform gap analysis to see which skills employees need; deliver training to fill the skills gap, implement an online security awareness program and validate through periodic tests. More advanced controls include: using security assessments for mission-critical roles, using real-world examples where possible, to measure mastery or identify skills gaps.
10. **Secure Configurations for Network Devices such as Firewalls, Routers & Switches**	The control objective is to establish, implement and actively manage the security configuration of the network infrastructure using a rigorous configuration management and change control process.	Basic controls include: documenting the security configuration of firewall, router and switches and comparing against standard secure configurations defined for each type of network device; documenting all new configurations rules that allow traffic to flow through network security devices; installing the latest version of security-related updates; using automated tools to verify standard device configurations and detect changes; using two-factor identification and encryption. More advanced configuration controls involve separate VLANS for the business use of that network or entirely different physical connectivity for management sessions for network devices.
11. **Limitation and Control of Network Ports, Protocols & Services**	The control objective is to manage ongoing operational use of ports, protocols and services on networked devices in order to minimize windows of vulnerability.	Basic controls include: apply host-based firewalls or port filtering tools on end systems with a default-deny rule that drops any traffic not explicitly allowed; keep all services up to date and uninstall/remove unnecessary components, ports, protocols or services not needed for business needs; operate critical services on separate machines; verify any server visible from the Internet or an untrusted network and move those not required for business purposes to an internal VLAN or a private address. More advanced controls including placement of application firewalls in front of any critical servers to verify and validate traffic going to the server.

Control Families	Objective	Examples
12. **Controlled Use of Administrative Privileges**	The control objective is to manage the assignment and configuration of administrative privileges on computers, networks and applications.	Basic controls include: configure all administrative passwords to be complex; utilize access controls lists to ensure that administrative accounts are only used for system administration activities with separate password for non-administrative accounts; restrict administration privileges; change all default passwords on new systems; ensure that all service accounts have complex passwords that are changed on a regular basis; configure operating systems to prohibit password re-use within six month time frame; configure systems to issue a log entry and alert when administrative accounts are added or deleted or for unsuccessful logins; use passwords should be hashed or encrypted in storage and should only be readable with super-user privileges. More advanced controls include: multifactor authentication for all administrative access and automated tools to inventory all administrative accounts and validate that privileges were authorized by a senior executive.
13. **Boundary Defense**	The control objective is to manage the flow of information between networks of differing trust levels with a focus on security-damaging data.	Basic controls include: deny communications with known malicious IP addresses or whitelist trusted sites, require all remote login access to use two-factor identification; design network perimeters so that all traffic muss pass through at least one DMZ network; all remote log-ins to internal network should be managed by the enterprise, with remote control of their configuration, installed software and patch levels. More advanced controls include: scanning for back-channel connections that bypass the DMZ; networked IDS sensors to detect unusual attack mechanisms; network-based IPS devices to block known bad signature or attack behavior; internal network segmentation to limited traffic by subcontractors, vendors or bad actors; configure firewall to identify TCO sessions that last an unusually long time; deploy NetFlow collection and analysis to DMZ network.

Control Families	Objective	Examples
14. **Maintenance, Monitoring & Analysis of Audit Logs**	The control objective is to collect, manage and analyze audit logs of events that could help detect, understand or recover from an attack.	Basic controls include: two synchronized time sources to ensure that timestamps in logs for all servers and network equipment are consistent; adequate space for log storage that it does not fill up between rotation intervals; log retention policy to ensure logs are kept for longer than it takes to detect an attack; biweekly reports on log anomalies; ensuring that log collection system does not lose events during peak activity and validating log setting for each hardware device and installed software. More advanced controls include: configuring network boundary devices to log all traffic to the device; ensuring that logs are written to write-only machines or dedicated logging servers; monitoring for service creation events and enabling process tracking logs; deployment of log analytic tools to aggregate and consolidate logs for correlation and analysis.
15. **Controlled Access Based on the Need to Know**	The control objective is to manage and secure access to critical assets (information resources, systems) according to a formal determination of individuals, computers or applications that have a need and right to access these assets.	There are no basic controls for this family. Advanced controls include: separating sensitive information on separate VLANs and encrypting all communications containing sensitive information; segmenting the network based on trust levels of the information stored on the servers and encrypting information flowing to lower trust networks; detailed audit logging for access to non-public data and special authentication for sensitive data.
16. **Account Monitoring & Control**	The control objective is to manage the life-cycle of system and application accounts — their creation, use, dormancy and deletion.	Basic controls include: disable any account that cannot be associated with a business process and owner; ensure that all accounts have an expiration date; establish a process for revoking system access accounts and disable accounts immediately upon termination of a contractor or employee; monitor accounts to determine dormancy; automatically log-off users after a standard period of inactivity; configure screen locks on unattended workstations; monitor attempts to access deactivated accounts; configure all systems to encrypt transmitted passwords. More advanced controls include: automated reports that included a list of lock-out accounts, disable accounts, outdated passwords; centralized authentication for all network and security devices; user profiles that establish typical usage and reports on atypical activity; multi-factor authentication for accounts with access to sensitive data or systems.

Control Families	Objective	Examples
17. Data Protection	The control objective to prevent data exfiltration, mitigate the effects of exfiltrated data and ensure the privacy and integrity of sensitive information.	Basic controls include: identify sensitive information that requires encryption or integrity controls; review cloud provider security practices for data protection; deploy approved hard drive encryption software to mobile devices or systems that hold sensitive data; verify that cryptographic devices and software are configured to use publicly-vetted algorithms; block access to known file transfer and e-mail exfiltration websites. More advanced data protection controls include: move data between networks using secure, authenticated and encrypted mechanisms; define roles and responsibilities related to encryption keys; deploy an automated tool on network perimeters to monitor sensitive information, keywords etc; conduct automated and periodic scans of server machines to determine whether sensitive information or personally identifiable information is resident on the system; configure systems such that they cannot write to USB tokens or hard drives; where USB devices are needed, configure systems to allow only specific USB devices to be accessed; perform annual review of algorithms and key lengths in use for data protection; monitor all traffic leaving the organization and detect unauthorized use of encryption.
18. Incident Response & Management	The control objective is to protect the organization's information as well as its reputation, by developing and implementing an incident response infrastructure to detect an attack, contain the damage, and restore the integrity of the network and systems.	Basic controls include: ensure written incident response procedures; assign job titles and duties to specific individuals; define management personnel who will support incident-handling process. More advanced controls include: organization-wide standards and mechanisms to report anomalous events to the incident response team; information on third party contact information to report a security incident; periodic incident scenario sessions to ensure that incident handling teams understand current threats and risks.
19. Secure Network Engineering	The control objective is to make security an inherent attribute of the enterprise by designing features that allow high confidence systems operations while denying or minimizing attack opportunities.	Basic controls include: deploy domain name systems in a hierarchical structure fashion with all internal network client machines configured to send requests to Intranet servers; design the network using a minimum of a three tier architecture (DMZ, middleware and private network); use a DMZ for any system accessible to the Internet. More advanced controls include: segment the enterprise network into multiple, separate trust zones and engineer the network for rapid deployment of new access control lists, rules, signatures, blocks, blackholes and other defensive measures.

Control Families	Objective	Examples
20. Penetration Tests & Red Team Exercises	The control objective is to test the overall strength of an organization's defenses by simulating the objectives and actions of an attacker.	Basic controls include regular external and internal penetration tests; clear goals for the penetration test with blended attacks targeting a particular machine or assets. More advanced controls include: tests for the presence of unprotected system information or artifacts; use of vulnerability scanning and penetration testing tools in tandem; periodic Red Team exercises to test organizational readiness; scoring methods to compare readiness results over time; a test bed that mimics a production environment for specific penetration tests, particularly against SCADA or other control systems.
21. Organization/ Governance	The control objective is to ensure a governance capability to develop and implement cybersecurity policy.	Basic controls include: assignment of cybersecurity risk management responsibilities; inclusion of cybersecurity in risk management plan; cybersecurity policy that is patterned after international standards; flow-down of cybersecurity policies to suppliers or third parties with whom sensitive information is shared. More advanced controls include: verifying that suppliers or third parties.
22. Mobile Device	The control objective is to limit the risk introduced by mobile devices into the network.	Basic controls include: assuring that all mobile devices have access controls in the devices, configuration management to enforce policies provided by a centrally managed infrastructure, and the ability by the company to remotely wipe the device.