
Stephanie Shankles, Booz Allen Hamilton
Michele Moss, Booz Allen Hamilton
Jed Pickel, Microsoft’s Trustworthy Computing group
Nadya Bartol, Utilities Telecom Council

Abstract: An increasingly distributed and global Information and Communication Technology (ICT) supply chain brings challenges to U.S. Government and industry. Identifying and mitigating risks involves looking beyond your organization and understanding and managing risks caused by the lack of visibility in the ICT supply chain. Recent research indicates that current ICT supply chain risk management practices tend to have a tactical focus motivated primarily by compliance rather than a strategic integrated approach. However, there are a number of existing international standards and several under development that when used in combination will help this problem. Using these standards together will provide a security assurance process for information security governance, software development, Supply Chain Risk Management (SCRM), and should result in reducing ICT supply chain risk.

Challenges in Today’s Global ICT Marketplace

ICT supply chain risk management covers both software and hardware. Several recent industry reports focused primarily on software and on the general state of information security provide insights into current ICT supply chain practices, and what motivates their selection:

- Software Security: Think Big, Start with What Matters, 2009 The Burton Group [1].
- Global Information Security Workforce Study, 2011 Frost & Sullivan and (ISC)2 [5].
- Software Integrity Controls, 2010 SAFECode [6].
- Assessing SCRM Capabilities and Perspectives of The IT Vendor Community: Toward a Cyber-Supply Chain Code of Practice, 2010 University of Maryland [7].
- Verizon and Secret Service (USSS) - Data Breach Investigations Report, 2010 and 2011 [8][9].

Together, these reports present the following key findings in Table 1.

Although each report is focused on different aspects of information security and therefore touches on different aspects of ICT supply chain security, they share a common message that holistic processes are needed to mitigate risks. Table 2 summarizes the results of three studies, which while conducted at a different level of detail, presented similar conclusions.

It is evident from the studies’ results that to advance the state of the software security practice, stakeholders across an organization will need to bridge the communication gap with the purpose of effectively balancing the executive priorities and the implementation of operational, technical, and management practices for software security and supply chain.

The Enterprise Strategy Group study [2] identified that over 40% of the surveyed organizations trust their developers to know how to develop secure software. Several key trends emerged from this and other studies appear:

1. Only 47% of acquirers are performing acceptance testing of third party code. As a result, vulnerabilities in the code are not identified until the code is in production and organizations that acquired this software are left with the consequences. While the problem originated in the software supply chain, the acquirers have to address the risk.

2. Compliance requirements to run scans of the operations environment result in the identification of code level vulnerabilities. Subsequently, the realization of insecure coding practices is not identified as an issue until the operations and maintenance phase of the lifecycle, when it is more difficult and costly to fix. Again, the problem that originated in the software supply chain is left up to the acquirer to address.

3. Shifting from responding to vulnerabilities identified during operations to preventative practices in technology acquisition and development takes time and effort (potentially increasing time to deliver and cost of initial product—even though, this cost has been demonstrated to be less than the lifecycle sustainment costs when fixed later). With 46% of respondents using a development method, the foundation is in place for a coordinated approach to maintaining legacy technology and minimizing the impact of security incidents.

ICT SCRM Practices

The University of Maryland (UMD) and the Enterprise Strategy Group conducted studies focused on procedures that organizations use to manage security and risk in their supply chains for ICT products and services. Supply chain risk management is one of the initiatives in the United States Comprehensive National Cyber Security initiative. As such, it has been the focus of discussion and study by a number of organizations. However, the practice of securing ICT supply chains is still in its infancy and is often a misinterpreted problem. The September 2011 article, “Renewable Industry in Turmoil Latest Sign: American Superconductor Accuses Chinese Firm—Its Biggest
Customer—of Espionage” in the Wall Street Journal highlights [10] several facets of the supply chain challenge that involved a prominent American wind turbine manufacturer. Proprietary software was stolen and given to a major Chinese competitor. An affiliate of the competitor was a major Chinese parts supplier to the American manufacturer Superconductor. It appears that the American manufacturer’s supplier was intentionally providing them with faulty parts and components. Not only was American Superconductor a victim of a malicious insider, they were also the victim of supply chain tampering. This challenge will grow as large and small organizations operate in increasingly complicated and globally dispersed supply chains.

### Key Findings

<table>
<thead>
<tr>
<th>What ICT supply chain practices organizations currently employ?</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Security practices surrounding software development are tactical in nature and do not address software security risks in a strategic manner.</td>
</tr>
<tr>
<td>▪ Supply chain risk management practices are tactical and are not addressed in a strategic manner.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What informs and motivates the selection of ICT supply chain processes?</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ The largest motivator for secure software development practices is compliance</td>
</tr>
<tr>
<td>▪ Lack of leadership support and resistance to changing existing software development practices is a barrier to the adoption of secure development methodologies.</td>
</tr>
<tr>
<td>▪ To advance the state of the software security practice, stakeholders across an organization will need to bridge the communication gap to effectively balance the executive priorities and the resources needed for the implementation of operational, technical, and management practices for software security and supply chain.</td>
</tr>
<tr>
<td>▪ 40% of organizations surveyed do not employ a secure software program because they trust their developers know how to develop secure software and/or don’t believe they have a security issue.</td>
</tr>
</tbody>
</table>

### Table 1:

<table>
<thead>
<tr>
<th>VDBR (Verizon)</th>
<th>Executive Perspective (Ernst &amp; Young)</th>
<th>Security Professional Perspective (Frost)</th>
<th>Common Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ 96% of breaches were avoidable through simple of intermediate controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Approximately half of the breaches utilized hacking or malware</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Increase in risk due to social networking, cloud computing and personal devices in the enterprise</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Data leakage is the primary concern for organizations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ New technologies are being deployed without adequate security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Application vulnerabilities are the #1 threat to organizations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>▪ Implement essential security practices (such as access control, network management, secure development, and log management/analysis) to mitigate the risk of a data breach and loss of sensitive data</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 2:
“American Superconductor Accuses Chinese Firm—Its Biggest Customer—of Espionage”

**INCIDENT:**
An employee of American Superconductor Corporation working in Austria is charged with stealing and modifying valuable software that controls turbines. The employee gave the software to Sinovel Wind Corporation, the Chinese company that is under contract with American Superconductor. Sinovel then passed it on to an affiliate, a fierce competitor of American Superconductor, who then repackaged it and sold it back to Sinovol at a very low cost.

**IMPACT:**
The stolen software has already appeared in turbines sold by Sinovel in China. It has given the Chinese valuable intellectual property and may lead to huge financial losses for American Superconductor. The company has gone from $30 a share early in the year to about $6 a share in September, falling sharply on the news of legal action.

**MITIGATION:**
Austrian authorities confirmed that they have arrested the employee and he is cooperating. American Superconductor is seeking criminal redress through Chinese and Austrian courts and the Beijing Arbitration Commission. They claim they are owed $250 million for breach of contract claim.

---

**Common Development Practice:**
The RuggedCom Operating System (ROS) contains a vulnerability that could allow an authenticated, remote attacker to access sensitive information on a targeted device. The vulnerability exists because the RSA private key infrastructure (PKI) for SSL communications between an affected device and the user is hard-coded (visible) in the affected software. An authenticated, remote attacker could exploit this vulnerability by reverse engineering the key from the affected software.

**Operational Impact:**
The vulnerability was discovered in smart grid networking devices produced by industrial networking equipment manufacturer RuggedCom. RuggedCom manufactures ethernet switches, network routers, wireless devices, serial servers, media converters and other communications equipment for use in harsh electrical and climatic environments like those found in electrical power substations, oil refineries, military installations or roadside traffic control cabinets.

**Risk:**
The vulnerability allows an attacker to decrypt any SSL-based communications between an end-user’s web page and the RuggedCom device. In addition, the hard-coded private key could be used in a man-in-the-middle (MITM) attack to impersonate a RuggedCom device undetected. A successful exploit could lead to the loss of system integrity and lead to additional attacks. Attackers could access power station communications, intercept sensitive data and communications, and even potentially take control of critical infrastructure systems.

---

Source: Don Davidson, DOD-CIO

---

http://online.wsj.com/article/SB10001424053111903374004576578971052370768.html

Similar to the security practices surrounding software development, currently used ICT supply chain risk management practices are also tactical and are not addressed in a strategic manner. For example, procedures that allow organizations to understand activities of suppliers, such as auditing vendor practices, are rarely used. When audits are used, organizations rarely allow those results to influence procurement decisions.

In addition to identifying that about 40% of the organizations surveyed do not employ a secure software program because they trust their developers know how to develop secure software and/or do not believe they have a security issue, the Enterprise Strategy Group study [2] also indicated that most development efforts are not employing essential security practices. The Verizon Data Breach Report identified similar issues.

According to the UMD study [7], there is a divide between small and large companies with regard to employing security measures and small companies are falling behind. However, the study findings suggest that incentives can lead to positive changes in this area. UMD research indicates that smaller organizations are highly motivated to use government cyber-SCRM practice guidelines.

There is a divide between small and large companies with regard to employing security measures and small companies are falling behind. However, the study findings suggest that incentives can lead to positive changes in this area. UMD research indicates that smaller organizations are highly motivated to use government cyber-SCRM practice guidelines.

The Overview layer in the figure depicts three overview standards that address the overall information security management (ISO/IEC 27000), information security in supplier relationships (ISO/IEC 27036-1), and application security (ISO/IEC 27034-1). Collectively these standards provide the fundamentals and vocabularies for these three disciplines. The Requirements layer depicts the two relevant requirements standards. ISO/IEC 27001 provides requirements for managing information security for the enterprise using a risk-based approach. ISO/IEC 27036-2 provides requirements to be used to protect enterprise information when working with suppliers or acquirers. Finally, the Guidance layer depicts the guidance standards associated with the requirements standards above. ISO/IEC 15288/12207 (Systems and software engineering—System lifecycle processes and Systems and software engineering—Software lifecycle processes) acknowledges integration of both ISO/IEC 27036 and ISO/IEC 27034 with system and software engineering standards. ISO/IEC 27036-3 provides specific guidance on ICT supply chain security in addition to the requirements in ISO/IEC 27036-2. ISO/IEC 27002 provides guidance for implementing security controls selected as a result of a risk assessment required by 27001. It should be noted that of these standards, ISO/IEC 27036 is in draft, while the rest are published standards. ISO/IEC 27001 and 27002 are currently under revision. These standards provide processes, controls, and practices for resolving many of the issues identified earlier.

**International Standards Environment and ICT SCRM**

The issues and challenges identified in the reports can be addressed by applying several existing and emerging international standards. Figure 4 illustrates the relationship between existing and emerging ISO standards that provide the framework for addressing ICT SCRM concerns evident from the various studies.
Information Security Management Governance

The ISO/IEC 27000 family of standards provides a number of standards for establishing and implementing an information security management system. Specifically, ISO/IEC 27001, Information Security Management System Requirements, provides a governance framework for information security. Implementing this framework will help gain leadership support for approaching the challenges of today’s global marketplace such as implementing appropriate operational, technical, and management practices for software security and supply chain.

ICT Supply Chain

While there are a number of published standards that can help organizations manage information security and associated risks, none of those currently published standards provides guidance on how to protect an organization’s information security interests in a relationship between acquirers and suppliers. ISO/IEC 27036 which is currently in draft, provides an approach for protecting sensitive enterprise data within the context of acquiring and supplying products and services. This multipart standard covers managing the information security aspects of a portfolio of supplier relationships, as well guidance for how to manage individual supplier relationships. The standard provides requirements that cover a broad variety of products and services, as well as context-specific guidance. Specifically, Part 3 focuses on ICT supply chain security.

The standard introduces a number of requirements and concepts that while not new in supply chain and sources contexts, are new in the information security context:

- Having a registry (inventory) of all suppliers.
- Assigning responsible individuals to manage information security aspects of relationships with each supplier.
- Assessing the criticality of such relationships and associated risks and using this criticality to prioritize supplier relationships and associated security requirements.

- Having a minimal set of information security requirements applicable to any supplier relationship.
- Monitoring the information security aspects of supplier relationships.
- Ensuring protection of data and information when terminating those relationships.

Software Development Security Practices

Secure software development practices are important to supply chain security risk management efforts. The Forrester study referenced earlier in this article provides a good basis for understanding potential risks from software development process gaps. Results of the study are concisely summarized in the statement: “While a majority of organizations have implemented some form of application security measures, very few have put in place an end-to-end strategic approach that incorporates security throughout the software development lifecycle.” The supply chain implication is that reviewing a vendor’s secure development practices is an important step in managing supply chain risks.

This raises several important questions, such as: what a secure development process should include, how an organization should manage that process, and how a vendor’s process should be evaluated? An obvious start is to ensure that a vendor has a secure development process, that it incorporates techniques that address real-world security threats, and that the vendor’s organization is clearly committed to supporting that process. But what is the right approach to creating such a process? And what else should be considered? In November 2011 the International Standards Organization published part 1 of ISO 27034, an internationally recognized application security standard that may help simplify the answers to those questions. Currently Part 1: Overview and concepts is published and latter parts are still in development. ISO 27034-1 provides frameworks and a process that can help inform a vendor’s approach to build and operate a comprehensive application security program. The standard can
also help an organization validate and identify gaps within their current application security program. Additionally, the standard can help an organization implement aspects of ISO 27001 via the systematic approach to risk management shared by the standards. ISO 27034-1 includes an annex that demonstrates how an existing development process based on the Microsoft Security Development Lifecycle aligns to ISO 27034. This may help simplify an organization’s efforts to implement the standard.

An organization that has reviewed and is considering adoption of ISO 27034-1 is likely to be taking a strategic approach to software security and be applying relevant application security controls through all phases of their software development lifecycle. Consequently, ISO 27034 may be a helpful tool to simplify the process of managing supply chain risks by providing a standards based approach for understanding if vendors in your supply chain are taking a strategic and holistic approach to software security.

Conclusion

Modern supply chains have introduced greater risks to organizations. Globalization and the proliferation of technology around the globe have presented new significant threats to national security, economic security and protection of intellectual property (investment). The combination of international standards efforts described in this paper will help to provide a solid foundation for organizations to integrate an organizationally driven, risk based implementation of ICT SCRM practices.

Acknowledgements:

We wish to thank Don Davidson of the DoD for encouraging us to write this article and Ken Lyle of Booz Allen Hamilton for his assistance with analyzing the studies and identifying examples to include in the article.

REFERENCES
