Preliminary Survey Results: Initial Considerations and Conclusions

A Working Paper of the EastWest Institute Breakthrough Group

Increasing the Global Availability and Use of Secure ICT Products and Services

August 5, 2015

The EastWest Institute (EWI) is leading a Global Cooperation in Cyberspace Initiative to help make cyberspace more secure and predictable. As part of that initiative, EWI has established a Breakthrough Group that is working to enhance cybersecurity for governments and enterprises globally by enabling the availability and use of more secure information and communication technology (ICT) products and services. This group also strives to encourage global recognition of a set of principles that should characterize and help to drive the global ICT marketplace toward more secure products and services and greater transparency.

For providers in the ICT supply chain, the group is promoting the use of recognized and proven international standards and best practices that improve product and service integrity. For buyers of ICT, the group is working to leverage the demand side of the ICT marketplace toward greater security. It is encouraging buyers of ICT to be more informed and organized with like-minded buyers, and more consistent in the inclusion of security requirements. It is also working to foster the use of procurement practices that are founded on recognized and proven standards and best practices for secure ICT.

To this end, EWI requested input on a set of principles and a set of questions for buyers and providers that will provide practical guideposts for evaluating and enhancing the security of ICT products and services, which in turn can be used to seek international support by private organizations and governments for these principles and the transparent use of such standards and best practices.

The survey was launched on July 15, 2015. The preliminary results phase ended on August 5. Sixty-three responses were received. The survey remains open at https://www.surveymonkey.com/s/LLN975D. At EWI's New York Summit on September 9, 2015, an updated version of this report will be presented and discussed. The survey was distributed by EWI and the breakthrough group members to several diverse groups, including: government, research and standards bodies, think tanks, NGO's and private industry.

Survey Demographics

Respondents came primarily from companies or organizations with under one thousand employees.[1] The second largest percentage of respondents came from organizations with five to twenty thousand employees.[2] Similarly, organizations with over sixty thousand employees represented 13% of the respondents.

These numbers were unsurprising given that the largest percentage of respondents (25%) came from government organizations. The top five industries cumulatively make up 53% of respondents and are as follows:

Government—25%
Telecommunications—18%
Education—14%

NGOs—12%

Research and Standards—11%

Those that responded to the survey primarily categorized their organization role as an "expert/specialist" or "head of business unit or department" level.[3] There was an equal distribution among respondents from the "owner/executive/c-level," "CISO/CIO/CTO/CRO" and "manager" levels ranging from 11-14%.

The majority of survey respondents consider themselves to be primarily buyers of ICT.[4] An additional 23% consider themselves to be equally a buyer and supplier of ICT. Given that only 26% of respondents consider themselves to be primarily suppliers of ICT, it can be concluded that this survey was of greater initial interest to buyers than suppliers. This may help to explain the responses to how risk is approached and requirements are considered.

Findings for Assessing and Prioritizing Risk in the Supply Chain

1. The approach of assessing and prioritizing risk is primarily developed in house with additional and equal use of NIST 800-30, NIST Cybersecurity Framework and ISO 31000.[5]
2. Organizations take varied and often inconsistent approaches to assessing and prioritizing risk.
3. In some industries, an in-house approach coupled with a "build security in" focus is the primary method of assessing and prioritizing risk.[6]
4. Organizations are evenly split on whether they have or have not considered standards and/or accreditation programs. Following this, those that have considered standards and/or accreditation programs primarily reference ISO 27036 or NIST 800-161.[7]

---

[1] 60% based on survey results.
[2] 15% based on survey results.
[3] 40% for expert/specialist and 19% for head of business unit or department based on survey results.
[4] 52% based on survey results.
[5] 47% develop their approach in house. A relatively equal distribution of the other three is quantified by a range of 26-29%.
[6] For question 4, a detailed response from the "other" answer choice provided the background for this analysis.

5. Six percent of respondents could not identify with the question "Identify any of the following standards and/or accreditation programs related to supply chain that you have considered or been asked to consider by suppliers" due to general lack of knowledge or scope.
6. Organizations use multiple and varied resources to develop cybersecurity, software assurance and supply chain requirements. The top five are as follows:
    - ISO 27001- 45%
    - NIST CSF- 33%
    - ISO 27002- 30%
    - NIST 800-53- 21%
    - NIST 800-161- 21%
7. Many organizations indicated their support for other resources listed in the survey or identified additional resources that the breakthrough group had not initially considered for inclusion, which serves to highlight the diversity of resources available to and used by organizations. Additional resources that received support in the survey but did not make it into the top five include: COBIT, Germany's Information Security BSI standard; HIPPA, Huawei's Top 100 Requirements; ISO 27034, ISO 27036, The Open Group (O-TTPS) recently approved as ISO/IEC 20243; and PCII. Other resources that were write-ins by respondents include: COPPA (Children's Online Privacy and Protection Act); FERPA (Family Educational Rights and Privacy Act); OWASP OpenSAMM; SP 800-126 Revision2; NIST SP 800-51 Revision 1; and the ITU-T X. 1500 series.
8. Just under half of organizations feel that their procurement requirements provide an opportunity to drive the security of the market.[8] Equally many feel that their organizations' requirements do not provide an opportunity to drive the security market forward, with the specific limiting factors being their relative size and lack of situational knowledge.

Initial Considerations

1. What can this Breakthrough Group do to assist smaller and newer organizations that are interested in driving the security market forward?
2. What correlations could be made by looking at individual responses? In particular, correlations among specific industry approaches would become clearer.

Cybersecurity Requirement Categories

This Breakthrough Group asked respondents to rank the relative importance of 11 cybersecurity requirement categories to their organization. "Verification" was deemed the most important with "Laws and Regulations" following closely behind. The remaining requirements were evenly distributed in importance with a standard deviation of 1.36.

The average rankings are as follows:

1st – Verification
2nd– Laws and Regulations

---

[7] 52% have not considered a specific standards and roughly 48% have either considered or been asked to consider a standards and /or accreditation program. Given, that the question allows multiple results, an exact percentage would require examining individual questionnaires rather than the grouped data.
[8] 48% based on survey results.

3rd – Third-Party Supplier Management
4th – Delivering Services Securely
5th – Standards and Processes
6th/7th – Strategy, Governance, and Control
6th/7th – Research and Development
8th – Audit
9th – Issue, Defect, and Vulnerability Resolution
10th – Manufacturing
11th – Human Resources

The relatively equal importance of many of these categories, excluding verification and laws and regulations, was supported in the open response question: "Are there other questions you think should have been asked?" Additional responses asked this Breakthrough Group to consider:

- Public-Private partnerships in development and operations.
- Human Resources: Encouraging the training and preparation of educators as smart and informed consumers.
- Questions related to the choice and deployment of cybersecurity technology.
- Questions related to an organization's understanding of Advanced Persistent Threats, how you keep them out and their overall interplay with supply chain.

Initial Considerations

1. What additional categories of cybersecurity requirements should be considered for inclusion?
2. What does it mean that verification and compliance with laws and regulations are the primary drivers of cybersecurity across organizations?

Findings: Supply Side (i.e., what do suppliers of ICT products and services need to hear from their customers?)

This Breakthrough Group asked participants to evaluate the following supply side principles.

- Supply Side Principles—providers of ICT need:
    - An open market that fosters innovation and competition.
    - A level-playing field for ICT providers, regardless of locale.
    - Broader use of a set of scalable and proportionate standards and best practices for security and integrity.
    - Procurement processes that utilize fact-driven, risk-informed and transparent requirements.
    - Streamlined, agile, and scalable international standards and approaches to conformance.
    - A commitment by governments and ICT providers to avoid requirements or behavior that undermines trust in ICT (e.g., installing back doors).
- While all suppliers agree that these principles should be included, 50% felt that additional principles should be considered by this Breakthrough Group, including:

    - Big companies need to have a plan for securing the supply chain as they increase their outsourcing of tasks and projects.
    - Suppliers need to work in tangent with buyers to increase knowledge, concern, and communication regarding the threat landscape and supply chain vulnerabilities, in order to strengthen the acquisition process.
    - Verification and evaluations should be incorporated into SOPs and exercised in a transparent manner.
- The role of assessing cybersecurity risks and determining risk priorities is often conducted in part at the CISO and Risk Team levels.[9]
- Many supply-side-only organizations (vendors) assess risk at multiple levels.[10]
- The majority of suppliers, 83%, of ICT are concerned to some degree about the potential of incorporating third-party supplier components, which may include vulnerabilities; 50% are extremely concerned about this prospect.
- Among suppliers of ICT, there is greater concern for counterfeit components from third party suppliers than for vulnerable component representing a 2% increase in overall concern for third-party supplier that components could be counterfeit. [11]

Initial Considerations

1. What can be learned about the extent and remit of risk assessment for each level of the organization?
2. What strategies are vendors using to minimize risk from third-party suppliers?

Findings: Demand Side (i.e., what do buyers of ICT products and services need to ask their suppliers?)

This breakthrough group asked participants to evaluate the following demand side principles:

Demand Side Principles—buyers of ICT need:

- Tools and approaches to assess risk.
- A comprehensive understanding of lifecycle costs for ICT to inform decisions not only based on lowest initial costs but also on best overall value.
    - Methods to develop and implement consistent procurement requirements appropriate to assessed risks.
    - A set of providers recognized as conforming to international standards and best practices for product and service integrity.

All buyers agreed that these principles should be included, with some comments indicating that additional focus on education of buyers should be considered by this breakthrough group.

[9] 83%, for each, based on survey results
[10] This question allowed for multiple responses. With the exception of "Other" all answer choices were chosen at least 3 times.
[11] 86% based on survey results.

Initial Conclusions

1. The categories and questions posed in the survey (based on the Huawei "Top 100") generally align with the buyer and supplier organizations' security requirements, with some suggested additions or changes in emphasis to give greater recognition to governance and human factors.
2. Considerable ambiguity and lack of direction remains in the communication signals between buyer and seller for security requirements, with a great diversity of standards and ad hoc approaches in use.

A more detailed analysis of the survey results, including changes based on the larger sample size, will be presented and discussed at the New York Summit on September 9, 2015.