Survey Questions:

This survey is conducted by a research group at University of Toronto, Department of Computer Science. The methods you practice may vary from a project to another or have changed from past to the present. Please provide the overall and general approaches that you have been practicing over the past two years at you job. The questions mostly aim to study your own activities and practices, not the general practices employed by your team, unless the question explicitly asks about the general practices employed in your organization or by your team.

Please read all the answers before selecting a choice. For each question, check all answers that apply, unless otherwise indicated. If none of the answers apply, leave the question unanswered.

1. How do you describe the size of your company?
   i. Small company, up to 50 employees
   ii. Medium-size company, up to 500 employees.
   iii. Large-size company, up to 10,000 employees.
   iv. Very large company, over 10,000 employees.
   v. Don't know.

2. How do you describe your company's business?
   i. Software development
   ii. IT solution provider
   iii. Telecommunication
   iv. Consulting
   v. Manufacturing
   vi. Financial
   vii. Insurance
   viii. Government
   ix. Healthcare
   x. Transportation
   xi. Retail
   xii. Energy
   xiii. Other , please specify

3. In what field is your post-secondary or post-graduate education?
   i. Computer Science
   ii. Computer/Electrical Engineering
   iii. Business/Management
   iv. Other, please specify

4. How do you describe your role in your organization?
   i. Requirements Engineer
   ii. Product Manager
   iii. Business Analyst
   iv. Software Designer
   v. Enterprise Architect
   vi. Software Developer and Programmer
   vii. IT and Network Specialist
   viii. Project Manager
   ix. Information Security Analyst
   x. Marketing
   xi. Other, please specify

5. Have you had any computer security training?
   i. Yes, as part of my formal education.
   ii. Yes, as part of the training I received at my job.
   iii. Yes, self study due to the job demands.
   iv. No.

6. At work, do you use security standards, guidelines, or checklists?
   i. No, but security standards and guidelines are used in our organization.
   ii. No, to my knowledge, we do not use any security standards and guidelines.
   iii. Yes, Common Criteria for Information Technology Security Evaluation
   iv. Yes ,ISO 17799 Security Standard
   v. Yes , NIST guidelines
   vi. Yes , SANS check lists and guidelines
   vii. Yes, Certified Information Systems Security Professional (CISSP) common body of knowledge
   viii. Other, please specify

7. How are the IT and software security practices regulated in your organization?
   i. Standardized across the organization.
   ii. Defined within each project or group.
   iii. Up to the individuals.

8. In your team or organization, does the person(s) responsible for requirements gathering elicit and document security requirements explicitly?
   i. No, in our projects (or organization), we do not deal with security requirements.
   ii. No, security issues are only dealt during the implementation phase or after the system being developed.
   iii. No, security requirements are discussed from early stages but are not documented, because it is assumed the implementation team will deal with security.
   iv. Yes, security requirements are gathered and documented in the early stages of the projects before the development starts.
   v. Don't know.

9. Do you use any modeling notation (such as UML or DFD) as part of the software development life-cycle?
   i. No, but in my opinion, we may need to consider using them.
   ii. No, in my opinion we do not need to use them.
   iii. No, we have used modeling notations in the past, but found they do not pay off.
   iv. Yes, we use an in-house notation developed in our organization
   v. Yes, we use common notation(s), please name the notation(s).

10. If you answered Yes to the previous question, please answer this question: When analyzing security requirements, what modeling notations do you use?
   i. We do not model security requirements.
   ii. We use the same modeling notations we mentioned in the previous question.
   iii. We have tailored our requirements modeling notations for dealing with security requirements.
   iv. We use different modeling notations for dealing with security requirements. … Please specify.

11. From the following list, please select the items if you have used in the past or you use them routinely in security requirements elicitation or to look for security solutions.
   i. Security-related text books
   ii. SANS or NIST guidelines
   iii. Standards such as ISO, IEEE, CISSP

iv. Software vendors' data sheets
v. Security design patterns
vi. CERT
vii. National Vulnerability Database (NVD)
viii. Common Vulnerability Enumeration (CVE)
ix. Common Vulnerability Scoring System (CVSS)
x. National/provincial security and privacy guidelines and standards

12. When dealing with a security issue or a security requirement, do you usually look for and analyze more than one alternative security solution? (For example, alternative security mechanisms for authentication are biometrics and passwords)

i. Yes, we usually look for multiple alternative solutions and then select one.
ii. No, we usually consider one single solution.

13. If you answered Yes to the previous question, please answer this question: How do you select one security solution or countermeasure when you have multiple options?

i. We usually select the most economical solution.
ii. We usually select the most secure solution even though it is not the most economical.
iii. We usually select a solution that balances out the security and financial costs.
iv. We usually consider multiple factors about solutions, such as their usability, the level of privacy and security they provide, costs, time to market, etc. Then we try to select a solution that satisfies as many as of these factors as possible.

14. Do you think security requirements and security mechanisms lead to trade-offs that you have to sacrifice some other requirements to obtain better security? [You can select multiple choices]

i. No, we can satisfy security requirements and other requirements simultaneously.
ii. Yes, security may have trade-offs with privacy
iii. Yes, security may have trade-offs with usability, user-friendliness, and ease of use
iv. Yes, security may have trade-offs with performance and efficiency
v. Yes, security may have trade-offs with financial costs
vi. Yes, security may have trade-offs with some functionalities and features
vii. Yes, security may have trade-offs with time to market
viii. Yes, security may have trade-offs with human resources

15. In your opinion, is it usually feasible to elicit preferences of users and customers about requirements? [Pick only one choice]

i. No, users and customers do not have a clear idea about their preferences and often change their mind, so it is not possible to extract accurate or useful preferences.
ii. Yes, by asking the users to rank the requirements from least important to most important one. For example, the most important one is ranked one and the second most important one is ranked two, etc.
iii. Yes, by asking the users to assign a number as the importance weigh of the requirements. For example, the most important one's weigh is 0.8, the next important one's weigh is 0.3, etc.

16. Do you look for and consider common attacks that have happened before to elicit security requirements and secure your systems?

i. Yes, we document security attacks that have happened and try that the attacks would not occur again.
ii. Yes, we consider well-known security attacks available in attack and vulnerability databases, or we ask security expert about common attacks.
iii. No, we do not consider attacks that have happened in the past.

17. Do you evaluate security risks associated with the system that you develop?
    i. We are aware that security risks exist, but we do not measure or evaluate risks explicitly.
    ii. Yes, we consider security risks, but usually do not evaluate them by quantitative measures. We consider qualitative labels for describing risks (such as Low, Medium, High)
    iii. Yes, we have explicit and quantitative methods for evaluating security risks. (Quantitative measures provide numerical or financial).

18. In your opinion, when evaluating the risk for potential attacks, which of the following methods is usually the most useful and feasible? (For example, suppose you are asked to evaluate the risk of denial of service attacks to your system) [Pick only one choice]
    i. Evaluating the risk as financial costs; e.g., the risk of the denial of service attack is approximately $ 25,000.
    ii. Evaluating the risk in terms of a number between 1 and 100; e.g., the risk of denial of service attack is 78 from the scale 1 to 100.
    iii. Evaluating the risk using the scale of 1 to 9, where 1 is the lowest and 9 is the highest; e.g., the risk of denial of service attack is 7 in the scale of 1 to 9.
    iv. Evaluating the risk using of labels of Low, Medium, High; e.g., the risk of denial service attack is medium.

Thanks for completing the survey. Your contribution to this research project is appreciated. If you have any question, concern, or feedback, please do not hesitate to contact us. We will be happy to share the results of the survey with you.

If you are willing to participate in an interview with the research team to provide more details about the requirements engineering practices in your projects, please contact the research conductor, Golnaz Elahi, via e-mail, gelahi@cs.toronto.edu.

Thanks and best regards, Merci et meilleures salutations