Auxiliary Material for the Study of Security Practitioners in Context: Their Activities and Interactions with Other Stakeholders Within Organizations

Rodrigo Werlinger[*], Kirstie Hawkey[†], Konstantin Beznosov[‡]

Laboratory for Education and Research in Secure Systems Engineering
lersse.ece.ubc.ca
University of British Columbia
Vancouver, Canada

Technical report LERSSE-TR-2009-01[§]

Last Modification Date: 2009/01/07

Revision: #2

Abstract

This technical report contains additional material for the the study, which investigated the context of interactions of IT security practitioners.

[*] rodrigow@ece.ubc.ca

[†] hawkey@ece.ubc.ca

[‡] beznosov@ece.ubc.ca

[§] This and other LERSSE publications can be found at lersse-dl.ece.ubc.ca

Contents

1 Questionnaire

1. Your name
2. Your business e-mail
3. What is your official job title?
4. What is your official job title?
5. What are your responsibilities?
6. What post-secondary education do you have? Please indicate the fields of study
7. What additional technical courses or other training have you had?
8. What sector is your organization in?
9. For each of the following how many do you do IT security management for?
   - users
   - machines
   - network devices
   - applications
   - databases
   - other devices or services
10. How many employees does your organization have at your location?
11. How many people in your location are involved in IT security?
12. What are the job titles of your colleagues who are involved in IT security at your location?
13. What is the job title of the person(s), including yourself, who coordinates IT security activities at your location?
14. What percentage of your time involves IT security?
15. What tools do you use?
16. Beyond this questionnaire, would you be willing to be interviewed in person about your experience with IT security? (The interview is expected to take about one hour and would be audio-recorded.)
17. If you will, please provide the names and business e-mail addresses of others who might be interested in answering this questionnaire.

2 Interview guide

2.1 Version 1

Job

- Please explain the general nature of your work from your point of view
- What are your Security Administration responsibilities?

People

- How do you interact with different types of people during the course of your work?
- That is, please explain what types they are, for example, users, managers, customers, or some other type.
- And, for each type, tell whether you use the telephone, email, instant message, go to meetings, or something else?
- Please give an example of a common interaction.
- Can you give an example of an indirect interaction, in which you get messages through bureaucratic or automated channels?
- For each of the types, what needs or topics are talked about?

Organization

- Is there anything special about your organization that makes IT security administration more difficult; for example, a rapid turnover of users, or special relationships with other organizations, or something else? Similarly, is there anything special about your organization that makes IT security administration easier?

Mis-communications: common, serious, find out, recover

- Regarding miscommunications, what would you say are the most common miscommunication situations?
- Can you give examples?
- What would you say are the most serious miscommunication situations?, Can you give examples?
- How do you find out that a miscommunication situation has occurred?, Can you give examples?
- What can be done to recover from miscommunications?, Can you give examples?

Tasks: arise, take, common, consult, prioritize, improve, error prone

- In the pre-interview questionnaire, you indicated that you usually do these kinds of activities. Do more activities come to mind?
- For each of the activities, please explain:
- How does it arise?
- What does it take to do it?
- Please give some examples of common activities.
- Who or what do you consult when you need to know something? Under what circumstances does this happen?
- Which of your activities do you do first, next, etc.? Please explain how you decide?
- Please give an example of a having to put something off in order to do something more urgent.
- Under what circumstances does this happen?
- What activities can be improved?
- What activities are the most error prone ?

Tools: select, like/dislike, discarded, features, wish for, error prone, serious, find out, recover

- Please talk about your tools, starting with the ones that you use most often down to the ones that you use the least often. For each tool, please explain:
- How you selected it from other similar tools.
- What you like about it.
- What you dislike about it.
- What tools do you no longer use and why?
- What features or properties to you wish for in your tools?
- What would you say are the most error prone security tools or features?
- What would you say are the most serious errors from a security tool?
- How do you find out that a tool has made an error?
- What can be done to recover from errors?

2.2 Version 2

Activities

- Actual duties/ official duties?
  - Develop policies?, Conduct risk analysis?, Design new projects?, Implement security controls? Solve end user security issues? Educate and train? Respond to security incidents? Respond to alarms?
- Organizational structure (centralized, distributed, .)
  - What are the positive/negative effects that you see of having this structure?
- Prioritization (typical day)
- Policies
  - What formal security guidelines/policies/architectures/models are in place?: Separation of duties, need to know.
  - What is the process to develop policies?
  - How are policies communicated?
  - What tools are used to enforce the policies?
- Organization and Security Incidents
  - Liabilities/risks specific to organization
  - What are the main challenges to implement security controls? (e.g., organization's culture, organization's structure, budget)
  - Have you experienced security incidents related to the liabilities/risks mentioned?
  - Skills used during security incidents
  - Knowledge and strategies during security incidents
  - Other resources? (tools)
- Tools
  - What tools are used?
  - When tools are used? (trying to map activities and tools)
  - How tools select it from other similar tools.
  - What you like/dislike about it?
  - What tools do you no longer use and why?
  - What features or properties to you wish for in your tools?
  - What would you say are the most error prone security tools or features?
  - What would you say are the most serious errors from a security tool?

  - How do you find out that a tool has made an error?
  - What do you do to recover from errors?

- Errors
  - Prevention (scars from past errors): what would you tell an apprentice are the places to exercise care; Informal policy (e.g., keys always in left hand pocket)
  - Detection
  - Recovery

- Communication
  - Who do you interact with? In which circumstances?
  - When is it necessary to interact with people outside of the organization?
  - What channels are used when interacting w/ different people?
  - What tools are used to interact?
  - How security tools support the communication of security controls/issues?
  - What types of reports are required? How are they generated?
  - What are the sources of misunderstandings during interactions?: Informal communications (e.g., not to follow procedures)? Lack of (timely) communication? Lack of context? Lack of shared sense of risk?; What are the consequences of miscommunications?
  - Common ground: what typo of information do you need to share?, How do they know that they are understood?; Likes about the way organization handles IT security; How organization could do a better job
  - Coordination (how to know when and where to do activities)
  - Group decision making

- Other
  - What differentiates doing IT security from other IT activities?
  - What makes IT security more difficult/easy than other IT jobs?
  - Inference from multiple sources (What does it look like?)
  - Pattern recognition
  - Construction achieved by using whatever comes to hand; patched together; mended
  - Distribution of knowledge - cross-cutting knowledge during incident response
  - Are there any constraints related to IT security communications/interactions?

2.3 Version 3

Overall Interview Guide (which pieces to use/focus on depends on background of participant)

Organizational context (beginning of EACH interview)

- Describe security management within your organization
  - Who is responsible for security within your organization?
  - What is the security management model (centralized, distributed, etc.)?
  - What are the positive/negative effects of this structure?
  - What do you like about the way organization handles IT security?
  - How could the organization do a better job?
- Can you describe the security policies in your organization (also probe for their role)
  - What formal (official, written) security guidelines/policies/architectures/models are in place?
  - What is done in practice?
  - What is the process to develop policies?
  - How are policies communicated?
  - How are security-related policies enforced?
- What security risks/challenges do you perceive to be important for your organization?
  - What security incidents has your organization experienced as a result of these risks/challenges?
- What challenges do you perceive in implementing security controls in your organization?
  - Do you think this is different from other types of organizations? (Probe for effects of organization type, organization culture, organization structure)

Activities (EACH interview)

- What is your role within the organization? (get overall role, lead into security specific activities)
  - Actual duties/ official duties (Let them talk, probe anything not on list to confirm that omissions are true negatives)
    - ∗ Perform and respond to security audits on the IT infrastructure?
    - ∗ Develop security policies?
    - ∗ Design and revise security services or projects?
    - ∗ Implement security controls?
    - ∗ Solve end user security issues?

        - ∗ Educate and train?
        - ∗ Respond to security incidents?
            - · Skills, knowledge and strategies, resources (tools) used
        - ∗ Mitigate new security vulnerabilities?

- Prioritization (typical day)

Security Tools (EACH interview)

- What tools are used for the various activities?
- Do you use ever use tools in combination? What order do you use them in?
- How are tools selected from other similar tools.
- How do you use tool X and what do you like/dislike about it? (if possible, get them to show the interface and probe their view of the functionality/usability afforded by the tool)
- What tools do you no longer use and why?
- What features or properties to you wish for in your tools?
- What would you say are the most error prone security tools or their features?
    - What would you say are the most serious errors from a security tool?
    - How do you find out that a tool has made an error?
    - What do you do to recover from errors?

Archiving (EACH interview)

- What kind of activities/incidents/interactions/communications do you document and how?
    - Documenting what was done (specific task), documenting what has happened (log files)
- Is there a need for recording/archiving of communications? In what circumstances?

Troubleshooting (EACH interview) (probe a specific incident with supporting artifacts (reports, log files notes) - if artifacts available, this topic gets priority over communication)

- Please draw a picture of a specific incident.
- How do you develop a picture of the problem in your head as you troubleshoot?
- When you are investigating an incident (security or otherwise), what is your main priority?
    - What types of information are you trying to find out?

  - What actions will you take?
  - Do you think that troubleshooting /archiving for security focuses more on what happened in the past (prosecution, plugging of security holes), while IT admin troubleshooting focuses more on the present and moving forward (what is the specific problem and how to get the system operational again)? Why?

- To what extent do you keep notes as you troubleshoot?
  - As you determine what to do next, how do you rely on knowledge in your head and on records that you or others have made?
  - What type of notes do you keep?
  - What type of data do you save? (system logs, reports, etc.)
  - How long do you keep the record?

- What knowledge and skills are necessary during troubleshooting?
  - Inference from multiple sources (What does it look like?)
  - Pattern recognition
  - Construction achieved by using whatever comes to hand; patched together; mended
  - Distribution of knowledge - cross-cutting knowledge during incident response

- When is it necessary to interact with people outside of the organization?

IT Security vs. General IT (probe in EACH interview) (Managers: overview/contrast of perceptions - IT practitioner w/ security duties or security practitioner w/ prior experience in general IT: probe for differences - Security practitioners: ask about their experiences and their perceptions of any differences)

- Metrics of Success
  - How do you know that you are successful in what you are doing?
  - What are the metrics of success used during a performance review?

- Rapidly evolving environment:
  - (IT) In your work day, how much do the non-security IT systems (e-mail, database, etc.) change?
    - How does this contrast with the security systems in use?
  - How much do you have to keep up-to-date on changes in technology?
  - How much do you have to keep up-to-date on changes in threats/legislation/business practices?
    - Do you check any news forums regularly? How often? Which ones?
    - Do you monitor an email lists regularly? Which ones?
    - How often to you react within a day to something that you've read?

    - How often do changes in practice/process occur?
    - What forces drive the changes (and need for education) in general IT systems? Does this differ for security-related systems and processes?
        - New technology?
        - Legal requirements?
        - Security incidents?
        - Installation problems? (security related?)
        - Business goals?
        - System architecture changes?
        - End users?

- Differences in focus
    - When conducting your activities (security or otherwise), do you feel that you need a wide overview of organization or are you able to take a more narrow focus on individual technologies/sections of the organization?
        - If indicate have a fairly narrow focus, ask them if this is a concern?
        - How much do you need to take into account the larger business goals and operations of the organization in your day-to-day IT tasks?
        - How much do you worry about how your actions are going to impact others within this organization?
        - How much do you worry about whether your actions are inline with the organizations goals?
        - Do you have a different focus when engaged in security activities than when engaged in the IT duties?
    - Do you think that others in the organization view your activities as being roadblocks to their goals or as enabling their goals?
        - How hard is it to get management buy-in?
            - Financial resources (Equipment purchases? New software?)
            - For procedural changes you suggest?
            - If you want to make changes, what slant would you put on it when you pitched it to management (increased security, updated technology to improve performance)?
        - How hard is it to get employee buy-in?
        - How does the organizational culture affect IT security in your organization? How does it affect IT in general?
    - What are specific constraints related to IT security communications/interactions?

Communication (If time, do within the context of the above activities, else briefly touch)

- Can you describe how often and with whom you interact?

- Tools to perform communications
  - What are the communications channels you use for these interactions? (email, chat, face to face, phone, reports)(Probe for the use of internal websites for communication)
  - How well do the security tools support interaction/integrate with the communication channels?
  - How do the end users understand the configuration done by security practitioners?
    - Does the tool give feedback?
    - Does the security practitioner need to provide explicit knowledge?
  - When is it necessary to interact with people outside of the organization?
  - Reporting
    - Can you describe a recent example of reporting?
    - What kinds of reporting tools do you use?
    - Are the tools flexible enough to create reports suitable for different stakeholders?
- Can you describe what kind of flexibility you need? (different content, different level of granularity)
- What information that is useful for prioritization do your tools/reports provide?
- What are the sources of misunderstandings during interactions?
  - Informal communications? (e.g., not to follow procedures)
  - Lack of (timely) communication?
  - Lack of context?
  - Lack of shared sense of risk?
- What are the consequences of miscommunications on security?
- Common ground
  - What type of information do you need to share?
  - How do they know that the information and your communication is understood?
- Coordination (how to know when and where to do activities)
- Group decision making