Survey on Information Security Countermeasures in Organizations

Implementation date: November 2008

Research Representative: Toshihiko Takemura (Postdoctral fellow, Research Center of Socionetwork Strategies, Kansai University)

This survey was conducted with a grant from the Okawa Foundation for Information and Telecommunications (FY 19)

Preliminary survey

Q1 What is your occupation?

1. Company executive/proprietor
2. Company worker (managerial)
3. Company worker (regular (non-managerial) employee)
4. Civil servant/teacher/organizational worker (managerial)
5. Civil servant/teacher/organizational worker (non-managerial employee)
6. Contract worker/dispatched employee --> End
7. Independent businessperson/self-employed --> End
8. Part-time worker --> End
9. Housewife --> End
10. Student --> End
11. Unemployed (including retired) --> End
12. Other --> End

Q2 Do you perform information security countermeasures (particularly network security countermeasures) at your organization?

1. Yes
2. No --> End

Q3 For what length of time have you performed this work?

1. Less than 1 year --> End
2. 1-3 Years
3. Over 3 years

Q4 What is your current position in your company?

1. President/CEO/COO
2. Executive/CIO
3. Department manager/division manager
4. Vice-president/section manager
5. Unit head/director
6. Other
7. No official position --> End

Q5 How good is your knowledge of your company's overall information security countermeasures particularly network security countermeasures?

1. Very good <GO Main Survey>
2. Reasonably good <GO Main Survey>
3. Not very good
4. Nonexistent

Main Survey

Q1 Please select the response that best describes the industry in which your company is active.

1. Food
2. Textiles/apparel
3. MFR Paper & Allied Products
4. Chemicals
5. Pharmaceuticals
6. Medical
7. Oil/gas
8. Iron and steel/metals
9. Machinery/precision equipment
10. Electrical equipment
11. Automobile manufacturing
12. Other manufacturing industry
13. Banking
14. Securities
15. Insurance
16. Other financial industry
17. Trading/distribution/wholesale

18. Retail
19. Railways/aviation
20. Transportation
21. Consulting/think tank
22. Mass communication/publishing/printing/advertising
23. Information processing/software/SE
24. ISP/CATV/xDSL
25. Other telecommunications/broadcasting
26. Other services
27. Construction/public works/real estate
28. Welfare
29. Education/research institutions
30. Power
31. Farming/mining/forestry/fisheries
32. Other: (   )

Q2 How many employees (including dispatched and part-time employees) are there at your company?

1. Less than 10
2. 10-49
3. 50-99
4. 100-299
5. 300-999
6. 1,000 - 2,999
7. 3,000 - 4,999
8. 5,000 - 9,999
9. 10,000 - 99,999
10. 100,000 - 149,999
11. 150,000 or more

Q3 What percentage of the employees of your company are dispatched or part-time?

1. Less than 5%
2. 5%-9%
3. 10%-14%
4. 15%-19%
5. 20%-24%

6. 25%-29%
7. 30%-34%
8. 35%-39%
9. 40%-44%
10. 45%-49%
11. 50% or more
12. Don't know

Q4 What is the annual turnover of your company?

1. Under 10,000,000 yen
2. 10,000,000 - 50,000,000 yen
3. 50,000,000 - 100,000,000 yen
4. 100,000,000 - 500,000,000 yen
5. 500,000,000 - 3,000,000,000 yen
6. 3,000,000,000 - 5,000,000,000 yen
7. 5,000,000,000 - 10,000,000,000 yen
8. 10,000,000,000 - 50,000,000,000 yen
9. 50,000,000,000 - 100,000,000,000 yen
10. Over 100,000,000,000 yen

Q5 Is your company a listed company?

1. Yes
2. No

Q6 To what extent do the activities of your company, in terms of their impact on the nation, social infrastructure or economic foundations, benefit the public? Please select an appropriate response from the options below.

1. Almost not at all
2. Little
3. More than other industries
4. Very much, given the nature of the industry

Q7 Of the business processes relevant to the main activities of your company, what percentage rely on information systems (including external systems) or the Internet? Please select an appropriate response from the options below.

	A small Percentage (under 25%)	A fair percentage (25% - 50%)	A high percentage (50% - 75%)	An extremely high percentage (over 75%)
Information systems (including external systems)				
Internet				

Q8 What percentage of the total sales of your company are represented by E-commerce (EC) sales? Please select one of the following options. Please include data for affiliated offices (branch companies, branch offices, sub-branches, etc.) in your calculations.

Here, EC indicates all transactions directly connected to sales, namely but not limited to logistics (arrangement of logistics, shipping, transportation management), provision of sales and services for which compensation is paid by customers (estimates, negotiations, sales planning, sales promotion, order management, customer information management, billing, payment), as well as clearing agency, money transfers, remittance, taking of deposits, loans, insurance, and other transactions in the financial sector.

1. 0%
2. 10%
3. 20%
4. 30%
5. 40%
6. 50%
7. 60%
8. 70%
9. 80%
10. 90%
11. 100%

Q9 How many information security personnel (excepting outsourced personnel) are there at your company? Please select an appropriate response from the options below.

1. 0
2. Less than 10
3. 10-49
4. 50-99
5. 100-299
6. 300-999
7. 1,000 to 2,999
8. 3,000 ~ 4,999
9. 5,000 ~ 9,999
10. Over 10,000

Q10 Please select all appropriates from the options below all the positions that exist at your company.

1. Chief Information Officer (CIO)
2. Chief security officer (CSO)
3. Chief Risk Officer (CRO)
4. Chief Privacy Officer (CPO)
5. Chief Information Security Officer (CISO)
6. Chief Compliance Officer (CCO)
7. None of the above <EX>

Q11 How many computers (including those rented or leased) are there at your company?

1. Under 10
2. 10-99
3. 100-999
4. 1,000 or more

Q12 How many servers (including those rented or leased) are there at your company?

1. Under 5
2. 5-9
3. 10-29
4. 30-49
5. 50-99
6. 100-499

7. 500-999
8. 1,000 or more
9. All servers are outsourced, thus 0
10. Servers not required, thus 0

Q13 What is your company's policy towards information security countermeasures? Please select the most appropriate response from the options below.

1. The company takes all such countermeasures in company --> Q15
2. Such countermeasures are outsourced at present, but the company hopes to take them in-house wherever possible in future --> Q15
3. Such countermeasures are taken in company at present, but the company hopes to outsource them wherever possible in future
4. The company outsources such countermeasures as a rule
5. The company has no policies such as the above --> Q15

Q14 Please answer this question if you answered<ANS Q13>to Q13. Please select from the options below all the responses corresponding to the reason for your answer.

1. To reduce costs
2. There are no appropriate personnel in-house
3. It is safer/better to enlist experts
4. An integrated security service is required
5. Other: please specify. FA [required]

Q15 Which of the following are true of your company's attitude towards information security countermeasures? Please select an appropriate response for each item.

	Very true	More true than false	More false than true	Totally false
They are an important management issue				
They are conducted as part of risk management				
They are essential to business operations				
They exist to protect the brand image and company performance from security-related damage				
They exist to ensure a certain level of quality in products and services offered to customers				

They exist as a means for the company to fulfill its social responsibilities				
They exist to enhance the competitiveness of the company (to distinguish the company's products and services from those of other companies)				
They are conducted as part of business process streamlining				
They exist as they are important for project activities				
They exist as they are necessary for adherence to laws and industry guidelines				
They exist so as the company does not fall behind other companies				
They exist in order to maintain trusting relationships with customers and trading partners				

Q16 Which of the following are true of your company's information security efforts? Please select an appropriate response for each item.

	Very true	More true than false	More false than true	Totally false
Information assets have been reviewed				
Business processes have been reviewed and revised				
Operations have been streamlined				
The company is now more highly estimated by business partners and customers				
The company's competitiveness has increased, with increased orders and the like				
Employee awareness of information security has improved				
Efficiency and productivity have fallen				
Understanding of the importance of risk management awareness has increased				

A commitment to information security has been obtained at management level				
Information security has come to be seen as a social responsibility of the company				
Sharing and use of information in the company has improved				
Information security efforts have become a consideration in selecting and entering into contracts with trading partners				
The total cost of security management has fallen				
The quality of products and services offered has risen				
Information security management capacity at the organization has increased				

Q17 The following questions refer to your company's efforts for information security management. Please select an appropriate response for each item.

	Conducted/adopted for two years or more	Conducted/adopted for up to years	Being investigated for possible use/adoption	No plans to use/adopt
Company-wide information security management				
Department-specific information security management				
Security countermeasures for business-critical matters				
Information security countermeasures for risk management purposes				

Information security management cycle such as the PDCA cycle				
ISMS or similar information security certification				
Information security basics including password rules thoroughly enforced				
Adherence to personal information protection law				
Information security insurance				
Information security countermeasures based on return on investment				
Business continuity plan				
Concrete steps in line with a business continuity plan				
Requirement of a certain level of information security from trading partners				
Information security audits(internal)				
Information security audits (external)				

Information security reports published / information security-relevant items added to CSR reports/etc.				
Formulation of security policy				

Q18 The following questions refer to your company's organizational/structural policies as regards information security management. Please select an appropriate response for each item.

	Conducted/adopted for two years or more	Conducted/adopted for up to years	Being investigated for possible use/adoption	No plans to use/adopt
A Chief Information Security Officer (CISO) appointed				
An information security department (CISO) established/clarified				
Information security staff appointed and their roles clarified				
Information security policy clarified by managers				
System to collect information on security holes (vulnerabilities)				
Training of information security officers				
Accumulation and sharing of in-house information security-related knowledge and know-how				

Information security incident response procedures/CSIRT (Computer Security Incident Response Team)				
Advancement of sharing and use of information in the company				
Information security education/training for employees				
Strengthening of employee management/surveillance & internal controls				
Employees' efforts towards information security included in performance assessments				
Physical security countermeasures				
Measures to prevent leaks of sensitive or important information				

Q19 How are computers shared at your company? Please select one response from the options below.

1. One or more computer per person
2. Several people use one computer
3. Several computers exist per section/division
4. Servers not used

Q20 How many email in-boxes are there at your company? Please select one response from the options below.

1. Less than 10
2. 10-99
3. 100-499
4. 500-999
5. 1000-4999

6. 5000 or more

Q21 What percentage of the email received at your company is spam mail? Please select one response from the options below.

1. 81% or more
2. 80%
3. 60%
4. 40%
5. 30%
6. 10%
7. Almost none

Q22 How are servers managed at your company? Please select an appropriate response for each item.

	Servers not used	In-house servers used	Outsourced servers used	Don't know
Web servers used				
Mail server				
File server				
DB server				
PROXY server				

Q23 Please select all appropriate responses from the options below concerning methods of information security cost-benefit analysis at your company.

1. ROI
2. NPV
3. IRR
4. ROSI
5. Other
6. Don't know
7. Such costs not calculated

Q24 What percentage of the information security activities of your company are outsourced? Please select one response from the options below.

1. 0%
2. 1-20%

3. 21-40%
4. 41-60%
5. 61-80%
6. 81% or more

Q25 What aspects of information security education does your company consider important? Please select all appropriate responses from the options below.

1. Security policy
2. Network security
3. Access control systems
4. Security management
5. Economic aspects of security
6. Security system configuration
7. Information forensics
8. Cryptography
9. Security investment/law
10. Other ( )

Q26 What technical information security countermeasures have been conducted at your company for over two years? Please select all appropriate responses from the options below.

1. Firewall
2. Anti-virus software
3. Anti-spyware software
4. Access control (for servers)
5. Intrusion Detection System (IDS)
6. Data encrypted during transmission
7. Saved files encrypted
8. General password authentication
9. Intrusion prevention system (IPS)
10. Log Management Software
11. Application firewall
12. IC Cards
13. One-time password
14. Forensic software
15. PKI

16. Biometric systems
17. Thin client
18. Email filtering
19. Quarantine Network System
20. VPN
21. Patch Management
22. Encrypted communications
23. URL Filtering
24. Wireless LAN Security Software
25. Other
26. Not conducted

Q27 What technical information security countermeasures have been conducted at your company for under two years? Please select all appropriate responses from the options below.

1. Firewall
2. Anti-virus software
3. Anti-spyware software
4. Access control (for servers)
5. Intrusion Detection System (IDS)
6. Data encrypted during transmission
7. Saved files encrypted
8. General password authentication
9. Intrusion prevention system (IPS)
10. Log Management Software
11. Application firewall
12. IC Cards
13. One-time password
14. Forensic software
15. PKI
16. Biometric systems
17. Thin client
18. Email filtering
19. Quarantine Network System
20. VPN
21. Patch Management

22. Encrypted communications
23. URL Filtering
24. Wireless LAN Security Software
25. Other
26. Not conducted

Q28 Please select all appropriate responses from the options below that you consider highly important for information security.

1. Internal Security Audits
2. Penetration Testing
3. Vulnerability assessment software
4. E-mail monitoring software
5. Web monitoring software
6. Information security education for general employees
7. Information security education for engineers
8. Manual maintenance
9. Improving employee security awareness
10. Strengthening information security policy
11. Other
12. No effective countermeasures

Q29 What problems are there with human resources for information security at your company? Please select all appropriate responses from the options below.

1. No in-house personnel have the necessary knowledge
2. Technology changes quickly, thus difficult to keep relevant personnel informed
3. Difficult to develop human resources
4. Few employees have the relevant skills, despite recruitment efforts
5. Difficult to measure the ability of technical personnel
6. The type of personnel required is unknown
7. Other (   )
8. No real problems
9. Don't know

Q30 How are information security countermeasures taught to executives and regular employees at your company? Please select all learning methods appropriate to each type of position.

	E-learning	Workshops and seminars	Dissemination of relevant information	No specific countermeasures taught
Executives (including top management)				
Full-time/permanent staff				
Junior employees/part-timers				

Q31 What information security training/education do full-time/permanent staff receive at your company? Please select all appropriate responses from the options below.

1. Technical aspects such as the workings of the Internet
2. The in-house information security system (contents of the security policy, etc.)
3. Security incidents and cases of damage arising thereof
4. The importance of and efforts to maintain in-house information security
5. Means to cope with security breaches such as virus infection or information leakage
6. Anti-virus countermeasures and methods and rules concerning patch management
7. Password rules and data backup strategies
8. Coping with social engineering (persons using false identities on the telephone, etc.)
9. Rules for controlling access to information assets
10. Rules for handling of confidential and important information/taking information out of the company
11. Security countermeasures for mobile computers and rules for use outside the company
12. Internal rules to protect personal information
13. Internal controls
14. Laws and guidelines on information security
15. Business continuity plan
16. Physical security
17. Other (   )

[Question display settings: [Q30-2-1] Or [Q30-2-2] Or [Q30-2-3]]

Q32 What information security training/education do junior employees/part-timers receive at your company? Please select all appropriate responses from the options below.

1. Technical aspects such as the workings of the Internet
2. The in-house information security system (contents of the security policy, etc.)
3. Security incidents and cases of damage arising thereof
4. The importance of and efforts to maintain in-house information security
5. Means to cope with security breaches such as virus infection or information leakage
6. Anti-virus countermeasures and methods and rules concerning patch management
7. Password rules and data backup strategies
8. Coping with social engineering (persons using false identities on the telephone, etc.)
9. Rules for controlling access to information assets
10. Rules for handling of confidential and important information/taking information out of the company
11. Security countermeasures for mobile computers and rules for use outside the company
12. Internal rules to protect personal information
13. Internal controls
14. Laws and guidelines on information security
15. Business continuity plan
16. Physical security
17. Other (   )

[Question display settings: [Q30-3-1] Or [Q30-3-2] Or [Q30-3-3]]

Q33 What issues and problems with information security currently exist at your company? Please select all appropriate responses from the options below.

1. Awareness of security among employees is poor
2. Information security incidents/problems may exist but are at present unclear
3. The sufficiency of the present security countermeasures is unknown
4. Countermeasures to cope with incidents are insufficient
5. It is difficult to assess the cost-benefit ration of information security countermeasures
6. It is difficult to see the losses incurred when an incident or problem occurs

7. No departments or employees are knowledgeable in information security
8. Countermeasures are taken on a departmental basis, hence difficult to introduce a company-wide system
9. It is difficult to see where to start with security countermeasures
10. The company doesn't know which information security company to rely on
11. Other (   )

Q34 What is your company's policy/thinking regarding investment in information security? Please select all appropriate responses from the options below.

1. Investment is made in security countermeasures if they are necessary to ensure business operations
2. Investment in security countermeasures is kept to a minimum to reduce costs
3. Company-wide information security investment is performed
4. Information security investment is performed on a departmental basis
5. Investment in security countermeasures is higher than that in other IT areas
6. Investment in security countermeasures is almost equal to that elsewhere
7. Investment in security countermeasures is performed to a level compliant with industry guidelines or equivalent to other companies
8. Investment is made in countermeasures deemed important by risk analysis or quantification of information assets
9. Investment is made in countermeasures calculated as potentially giving high return
10. Return on investment is not calculated, however investment is made in countermeasures thought to give high return
11. Expensive countermeasures are not taken, even if high return can be expected
12. Other (   )

Q35 How often have the following occurred at your company over the last two years? Please select all appropriate responses from the options below.

	No problems	Once	2-3 times	4-5 times	6 times or more	Don't know
Premeditated leakage of company information						
Premeditated leakage of personal information						

Accidental leakage of corporate information						
Accidental leakage of personal information						
Theft of information assets						
Unauthorized access by outside parties						
Unauthorized access by inside parties						
Virus/worm infection						
System shut down by DoS attack						
Botnet/spyware infection						
Phishing						
Password sniffing						
System delays caused by spam mail						
System intrusion						
Trap						
Data destruction						
Tampering with the website						
Theft of notebook computers, etc.						
Social engineering						
	No problems	Once	2-3 times	4-5 times	6 times or more	Don't know

Q36 How would your company be affected by information security-related damage? Alternatively, if such damage has been incurred, how was the company affected? Please select all appropriate responses from the options below.

1. Drop in sales
2. Loss of business confidence
3. Deterioration of brand image
4. Dealings with customers/trading partners halted
5. Damage to business through voluntary cessation of operations, etc. [[ok?]]

6. Penalties for violation of contractual obligations (from principal contractor companies)
7. Deprivation of third-party certification (such as privacy marks)
8. Impact on share prices
9. Customer defection
10. Other (   )

Q37 Are there any information security countermeasures you would like the government/municipalities to take? Please select all appropriate responses from the options below.

1. Legal system to crack down on infringements
2. Systematization of evaluation/classification of security firms
3. Standardization of qualifications of specialist information security personnel
4. Provision of funding for use of security services
5. Provision of funding for purchase of equipment/software
6. Provision of funding for employee training
7. Provision of information security lectures/seminars/training
8. Provision of various products and service information
9. Provision of information warning of viruses, security holes, etc.
10. Development of technology against viruses, security holes, etc.
11. Other (   )
12. Nothing in particular

Q38 How has information security management changed over the last two years at your company? Please select an appropriate response from the options below.

1. Become stricter
2. Become less strict
3. No particular change
4. Other (   )

Q39 What countermeasures would you consider desirable to ensure comprehensive in-house information management? Please select the five most appropriate responses from the options below. [Required (1-5)]

1. Participation of company managers in information security management
2. Implementation of information security training for employees
3. Clarification of the rules of internal information management

4. Tightening of access to company information
5. Sharing of information that should be managed in company
6. Internal network access management
7. Enhancement of network security countermeasures such as anti-virus software and patches
8. Clarification of rules on use of company computers and mobile phones
9. Penalties for employees violating information management rules
10. Use of an Information Security Management System (ISMS)/Privacy Mark certification, etc.
11. Publication by public institutions of information security management level of companies
12. Strengthening of rules and regulations on information security
13. Other (   )
14. Nothing in particular

Q40 What is the level of information security awareness among employees other than information security officers at your company? Please select an appropriate response from the options below.

1. Information security awareness is high, from top management to regular employees
2. Information security awareness is high from top to middle management, but low below this level
3. Information security awareness is high from top management to department manager level but low below this level
4. Information security awareness is high among top management only
5. Information security awareness is low among all personnel except information security officers

Q41 What security countermeasures are now under investigation at your company? Please select the five most important responses from the options below. [Required (1-5)]

1. Encryption of data and emails
2. Introduction of VPN
3. Introduction of anti-virus software
4. Introduction of anti-spyware software
5. Filtering of emails/web
6. Introduction of a firewall

7. Strengthening of OS/applications
8. Introduction of an intrusion detection system (IDS)
9. Introduction of a Web tampering detection tool
10. Introduction of biometric authentication tools
11. Introduction of PKI/digital certificates
12. Introduction of one-time password rules
13. Implementation of port scans
14. Implementation of vulnerability assessments (vulnerability analysis, pseudo-attacks, etc.)
15. Implementation of log analysis
16. Implementation of security audits/consulting
17. Implementation of risk analysis
18. Formulation of information security policy
19. Implementation of employee training
20. Other (   )