Information Systems Security Risk

11

There are a number of threats to contemporary information systems. These include the leakage and modification of sensitive intellectual property and trade secrets, compromise of customer-employee-associate personal data, disruptions of service attacks, Web vandalism, and cyber spying. Our culture has seen an explosion in social networking and use of cloud computing, to include work environments where employees can bring their own devices (BYOD) such as i-phones or computers to do their work. In principle, this allows them to work 24 hours a day 7 days a week. In practice, at least it allows them to work when they please anywhere they please. Information security is the preservation of information confidentiality, integrity, and availability. The aims of information security are to ensure business continuity, comply with legal requirements, and to provide the organization with a competitive edge (leading to profit in the private sector, more efficient administration in the public sector).

The objectives of information security risk management can be described as[1]:

1. Risk identification
2. Risk assessment (prioritization of risks)
3. Identification of the most cost-effective means of controlling
4. Monitoring (risk review).

Step 3 includes risk mitigation options of avoidance, transfer, or active treatment of one type or another. Three endemic deficiencies were identified:

1. **Information security risk identification is often perfunctory**, with failure to identify risks related to tacit knowledge, failure to identify vulnerability from interactions across multiple information assets, failure to identify indications of fraud, espionage, or sabotage, failure to systematically learn from past events, and failure to identify attack patterns in order to develop effective countermeasures.

D.L. Olson, D.D. Wu, *Enterprise Risk Management Models*, Springer Texts in Business and Economics, DOI 10.1007/978-3-662-53785-5_11

2. **Information security risks are commonly considered without reference to reality**.
3. **Information security risk assessment is usually intermittent** without reference to historical data.

Internal threats are also present. Some problems arise due to turbulence in personnel, through new hires, transfers, and terminations. Most insider computer security incidents have been found to involve former employees.[2] External threats include attacks by organized criminals as well as potential threats from terrorists.[3]

Frameworks

There are a number of best practice frameworks that have been presented to help organizations assess risks and implement controls. These include that of the international information security management standard series ISO2700x to facilitate planning, implementation and documentation of security controls.[4] In 2005 this series replaced the older ISO 17799 standards of the 1990s. The objective of the standard was to provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an information security management system. It continues reliance on the Plan-Do-Check-Act (PDCA) model of the older standard. Within the new series are:

- ISO 27001—specification for an ISMS including controls with their objectives;
- ISO 27002—code of practice with hundreds of potential control mechanisms;
- ISO 27003—guidance for implementation of an ISMS, focusing on PDCA;
- ISO 27004—standard covering ISMS measurement and metrics;
- ISO 27005—guidelines for information security risk management (ISRM);
- ISO 27006—Accreditation standards for certification and registration.

Gikas[5] compared these ISO standards with three other standards, two governmental and a third private. The Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996, requiring publication of standards for electronic exchange, privacy, and security for health information. HIPAA was intended to protect the security of individual patient health information. The Federal Information Security Management Act (FISMA) was enacted in 2002, calling upon all federal agencies to develop, document and implement programs for information systems security. The industry standard is the Payment Card Industry-Digital Security Standard (PCI-DSS), providing a general set of security requirements meant to give private organizations flexibility in implementing and customizing organization-specific security measures related to payment account data security. Table 11.1 gives PCI-DSS content:

Other frameworks address how information security can be attained. Security governance can be divided into three divisions: strategic, managerial and operational, and technical.[6] Strategic factors involved leadership and governance. These

Table 11.1 PCI-DSS

Principle	Requirement
Build and maintain a secure network	1. Install and maintain a firewall to protect cardholder data 2. Don't use vendor-supplied default passwords and security parameters
Protect cardholder data	3. Protect stored cardholder data 4. Encrypt cardholder data transmission over open public networks
Maintain a vulnerability management program	5. Regularly update and use anti-virus software 6. Develop and maintain secure systems
Implement strong access control	7. Restrict access to cardholder data by need-to-know 8. Assign unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly monitor and test	10. Track and monitor all access 11. Regularly test systems and processes
Maintain an information security policy	12. To address information security

involve sponsorship, strategy selection, IT governance, risk assessment, and measures to be used. Functions such as defining roles and responsibilities fall into this category.[7] The managerial and operational division includes organization and security policies and programs. This division includes risk management in the form of a security program, to include security culture awareness and training. Security policies manifest themselves in the form of policies, procedures, standards, guidelines, certification, and identification of best practices. The technical division includes programs for asset management, system development, and incident management, as well as plans for business continuity.

Levels of such a capability maturity model for information systems security can by[8]:

- Level 1—Security Leadership: strategy and metrics
- Level 2—Security Program: structure, resources, and skill sets needed
- Level 3—Security Policies: standards and procedures
- Level 4—Security Management: monitoring procedures, to include privacy protection
- Level 5—User Management: developing aware users and a security culture
- Level 6—Information Asset Security: meta security, protection of the network and host
- Level 7—Technology Protection & Continuity: protection of physical environment, to include continuity planning.

Information security faces many challenges, to include evolving business requirements, constant upgrades of technology, and threats from a variety of sources. Vendors and computer security firms send a steady stream of alerts about new threats arising from the Internet. Internally, new hires, transfers, and

terminations may be the germination of threats from current or former employees. There also are many changes in legal requirements, especially for those organizations doing work involving the government.

Security Process

As a means to attain information technology security, consider the following[9]:

Establish a Mentality To be effective, the organization members have to buy in to operating securely. This includes sensible use of passwords. Those dealing with critical information probably need to change their passwords at least every 60 days, which may be burdensome, but provides protection for highly vulnerable information. Passwords themselves should be difficult to decipher, running counter to what most of us are inclined to use. Training is essential in inculcating a security climate within the organization.

Include Security in Business Decision Making When software systems are developed, especially in-house, an information security manager should certify that organizational policies and procedures have been followed to protect organizational systems and data. When pricing products, required funding for security measures need to be included in business cases.

Establish and Continuously Assess the Network Security audits need to be conducted using testable metrics. These audits should identify lost productivity due to security failures, to include subsequent user awareness training.

Automation can be applied in many cases to accomplish essential risk compliance and assessment tasks. This can include vulnerability testing, as well as incident management and response. The benefits can include better use of information, lower cost of compliance, and more complete compliance with regulations such as Sarbanes-Oxley and HIPAA.

Table 11.2 provides a security process cycle within this framework:

This cycle emphasizes the ability to automate within an enterprise information system context. A means to aid in assessing vulnerabilities is provided by the risk matrices we discussed in Chap. 2. Cyber-crime includes ransom-ware (where consumer computers are frozen until a ransom is paid), cyber blackmail (holding banks at ransom with threat to publish client data), on-line banking, Trojan horses, phishing, and denial of service, spying (governmental or commercial), as well as mass hacking for political or ideological reasons. Table 11.3 provides a risk matrix for this case[11]:

This matrix could be implemented by assigning responsibility for risk to the executive board for Red categories, to heads of division for Yellow, and to line managers for Green. Each of these responsibility levels could determine the extra

Table 11.2 Tracy's security process cycle[10]

Process	IT impact	Function
Inventory	Assets available	Access assets in hardware and software
Assess	Vulnerabilities	Automatically check systems for violations of risk policies based on regulatory and commercially accepted standards
Notify	Who needs to know?	Automatically alert those responsible for patch management, compliance
Remediate	Action needed	Automate security remediation by leveraging help desks, patch databases, configuration management tools
Validate	Did corrective actions work?	Automatically confirm that remediation is complete, record compliance and confirm compliance with risk posture policies
Report	Can you get information needed?	Give management views of enterprise IT risk and compliance, generate

Table 11.3 Risk tolerance matrix for cyber crime

	Negligible impact	Low impact	Significant impact	Major impact	Very severe impact
Almost certain	Green	Yellow	Red	Red	Red
Likely probability	Green	Yellow	Red	Red	Red
Possible probability	Green	Green	Yellow	Red	Red
Unlikely probability	Green	Green	Yellow	Red	Red
Rare probability	Green	Green	Green	Yellow	Red

mitigation measures suggested by their information technology experts to lower residual risk.

Best Practices for Information System Security

Nine best practices to protect against information system security threats can include[12]:

1. **Firewalls**—hardware or software, which block unallowed traffic. Firewalls do not protect against malicious traffic moving through legitimate communication channels. About 70 % of security incidents have been reported to occur inside fire walls.
2. **Software updates**—application vulnerabilities are corrected by patches issued by the software source when detected. Not adopting patches has led to vulnerabilities that are commonly exploited by hackers.

3. **Anti-virus, worm and Trojan software**—should be installed on all machines. Management policies to reduce virus vulnerability include limiting shareware and Internet use, as well as user training and heightened awareness through education can supplement software protection.
4. **Password policy**—users face a constant tradeoff between sound password structure and workability (the ability to remember). But sound password use is needed to control access to authorized users. Human engineering in the form of naïve acquisition of passwords by intruders continues to be a problem.
5. **Physical security**—including disaster recovering planning and physical protection in the form of locks to control access to critical system equipment. Trash management also is important, as well as identification procedures.
6. **Policy and training**—because many information system security risks arise due to unawareness, a program of enlightenment can be very beneficial in controlling these risks. The other side of the coin is policy, the adoption of sound procedures governing the use of hardware, e-mail, and the Internet. Policy and training thus work together to accomplish a more secure system operating environment.
7. **Secure remote connections**—ubiquitous computing creates the opportunity to vastly expand mobile computing connections, and thus make workers much more productive. In order to gain these advantages, good encryption techniques are required as well as sound authentication procedures.
8. **Server lock down**—limiting server exposure is a basic principle. Those servers linking to the Internet need to be protected against intrusion.
9. **Intrusion detection**—systems are available to monitor network traffic to seek malicious bit patterns.

Supply Chain IT Risks

Information technology makes supply chains work through the communication needed to coordinate activities across organizations, often around the world.[13] These benefits require openness of systems across organizations. While techniques have been devised to provide the required level of security that enables us to do our banking on-line, and for global supply chains to exchange information expeditiously with confidence in the security of doing so, this only happens because of the ability of information systems staff to make data and information exchange secure.

IT support to supply chains involves a number of operational forms, to include vendor management inventory (VMI), collaborative planning forecasting and replenishment (CPFR), and others. These forms include varying levels of information system linkage across supply chain members, which have been heavily studied.[14]

Within supply chains, IT security incidents can arise from within the organization, within the supply chain network, or in the overall environment.[15] Within each threat origin, points of vulnerability can be identified and risk mitigation strategies customized. The greatest threat is loss of confidentiality. An example would be a case where a supplier lost their account when a Wal-Mart invoice was

unintentionally sent to Costco with a lower price for items carried by both retailers. Supply chains require data integrity, as systems like MRP and ERP don't function without accurate data. Inventory information is notoriously difficult to maintain accurately.

Value Analysis in Information Systems Security

The value analysis procedure has been used to sort objectives related to information systems security.[16] That process involved three steps, which they described as:

1. Interviews to elicit individual values.
2. Converting individual values and statements into a common format, generally in the form of object and preference. This step included clustering objectives into groups of two levels.
3. Classifying objectives as either fundamental to the decision context or as a means to achieve fundamental objectives.

Once the initial hierarchy was developed, it was validated by review with each of the seven experts involved. Sub-objectives were then classified as essential, useful but not essential, or not necessary for the given decision context. Hierarchy clustering was also reviewed.

We will apply that hierarchy with the SMART procedure (also outlined earlier) to a hypothetical decision involving selection of an enterprise information (EIS, or ERP) system. Tradeoffs among alternative forms of ERP have been reviewed in depth.[17] The SMART method has been suggested for selecting among alternative forms of ERP.[18]

Tradeoffs in ERP Outsourcing

Bryson and Sullivan cited specific reasons that a particular ASP might be attractive as a source for ERP.[9] These included the opportunity to use a well-known company as a reference, opening new lines of business, and opportunities to gain market-share in particular industries. Some organizations may also view ASPs as a way to aid cash flow in periods when they are financially weak and desperate for business. In many cases, cost rise precipitously after the outsourcing firm has become committed to the relationship. One explanation given was the lack of analytical models and tools to evaluate alternatives.

ASPs become risky from both success, or conversely, bankruptcy. ASP sites might be attacked and vandalized, or destroyed by natural disaster. Each organization must balance these factors and make their own decision.[19]

ERP System Risk Assessment

The ideal theoretical approach is a rigorous cost/benefit study, in net present terms. Methods supporting this positivist view include cost/benefit analysis, applying net present value, calculating internal rate of return or payback. Many academics as well as consulting practitioners take the position that this is crucial. However, nobody really has a strong grasp on predicting the future in a dynamic environment such as ERP, and practically, complete analysis in economic terms is often not applied.

The Gartner Group consistently reports that IS/IT projects significantly exceed their time (and cost) estimates. Thus, while almost half of the surveyed firms reported expected implementation expense to be less than $5 million, we consider that figure to still be representative of the minimum scope required. However, recent trends on the part of vendors to reduce implementation time probably have reduced ERP installation cost. In the U.S., vendors seem to take the biggest chunk of the average implementation. Consultants also take a big portion. These proportions are reversed in Sweden. The internal implementation team accounts for an additional 14 % (12 % in Sweden). These proportions are roughly reversed in Sweden with training.

Total life cycle costs are needed for evaluation of ERP systems, which have long-range impacts on organizations. Unfortunately, this makes it necessary to estimate costs that are difficult to pin down. Total costs can include:

- Software upgrades over time, to include memory and disk space requirements
- Integration, implementation, testing, and maintenance
- Providing users with individual levels of functionality, technical support and service
- Servers
- Disaster recovery and business continuance program
- Staffing.

Qualitative Factors

While cost is clearly an important matter, there are other factors important in selection of ERP that are difficult to fit into a total cost framework. A survey of European firms in mid-1998 was conducted with the intent of measuring ERP penetration by market, including questions about criteria for supplier selection.[20] The criteria reportedly used are given in the first column of Table 11.4, in order of ranking. Product functionality and quality were the criteria most often reported to be important. Column 2 gives related factors from another framework for evaluating ASPs, while column 3 gives more specifics in that framework.[21]

While these two frameworks don't match entirely, there is a lot of overlap.

Table 11.4 Selection evaluation factors

ERP supplier selection (Van Everdingen et al.)	ASP evaluation (Ekanayaka et al.)	Ekanayaka et al. subelements
1. Product functionality	Customer service	1. Help desk & training
		2. Support for account administration
2. Product quality	Reliability, scalability	
3. Implementation speed	Availability	
4. Interface with other systems	Integration	1. Ability to share data between applications
5. Price	Pricing	1. Effect on total cost structure
		2. Hidden costs & charges
		3. ROI
6. Market leadership		
7. Corporate image		
8. International orientation		
	Security	Physical security of facilities
		Security of data and applications
		Back-up and restore procedures
		Disaster recovery plan
	Service level monitoring & management	1. Clearly defined performance metrics and measurement
		2. Defined procedures for opening and closing accounts
		3. Flexibility in service offerings, pricing, contract length

Multiple Criteria Analysis

An example is extracted here from the literature[22] to show the application of multiple criteria analysis technique in managing IT risks. The data in the example are altered to fit our analysis scope. The multiple criteria analysis was found useful when used together with cost-benefit analysis, which seeks to identify accurate measures of benefits and costs in monetary terms, and uses the ratio benefits/costs (the term benefit-cost ratio seems more appropriate, and is sometimes used, but most people refer to cost-benefit analysis). Because ERP projects involve long time frames (for benefits if not for costs as well), considering the net present value of benefits and costs is important.

Recognition that real life decisions involve high levels of uncertainty is reflected in the development of fuzzy multiattribute models. The basic multiattribute model is to maximize value as a function of importance and performance:

$$value_j = \sum_{i=1}^{K} w_i \times u(x_{ij}) \quad (1)$$

where w_i is the weight of attribute i, K is the number of attributes, and $u(x_{ij})$ is the score of alternative x_j on attribute i.

Multiple criteria analysis considers benefits on a variety of scales without directly converting them to some common scale such as dollars. The method (there are many variants of multiple criteria analysis) is not at all perfect. But it does provide a way to demonstrate to decision makers the relative positive and negative features of alternatives, and gives a way to quantify the preferences of decision makers.

We will consider an analysis of six alternative forms of ERP: from an Australian vendor, the Australian vendor system customized to provide functionality unique to the organization, an SAP system, a Chinese vendor system, a best-of-breed system, and a South Korean ASP. We will make a leap to assume that complete total life cycle costs have been estimated for each option as given in Table 11.5.

The greatest software cost is expected to be for the best-of-breed option, while the ASP would have a major advantage. The best-of-breed option is expected to have the highest consulting cost, with ASP again having a relative advantage. Hardware is the same for the four mainline vendor options, with the ASP option saving a great deal. Implementation is expected to be highest for the customized system, with ASP having an advantage. Training is lowest for the customized system, while the best-of-breed system the highest.

But there are other important factors as well. This total cost estimate assumes that everything will go as planned, and may not consider other qualitative aspects. Multiple criteria analysis provides the ability to incorporate other factors.

Perhaps the easiest application of multiple criteria analysis is the simple multiattribute rating theory (SMART). SMART provides decision makers with a means to identify the relative importance of criteria in terms of weights, and measures the relative performance of each alternative on each criterion in terms of scores. In this application, we will include criteria of seven factors: Customer service; Reliability and scalability, Availability, Integration; Financial factors;

Table 11.5 Total life cycle costs for each option ($ million)

	Australian vendor	Australian vendor customized	SAP	Chinese vendor	B-of-B	South Korean ASP
Software	15	13	12	2	16	3
Consultants	6	8	9	2	12	1
Hardware	6	6	6	4	6	0
Implement	5	10	6	4	9	2
Train	8	2	9	3	11	8
Total Cost	40	39	42	15	54	14

Table 11.6 Relative scores by criteria for each option in example

	Australian vendor	Australian vendor customized	SAP	Chinese vendor	B-of-B	South Korean ASP
Customer service	0.6	**1**	0.9	0.5	0.7	0.3
Reliability, Availability, Scalability	**1**	0.8	0.9	0.5	0.4	**0**
Integration	0.8	0.9	**1**	0.6	0.3	0.3
Cost	0.6	0.7	0.5	0.9	0.2	**1**
Security	**1**	0.9	0.7	0.8	0.6	**0**
Service level	0.8	0.7	**1**	0.6	0.2	**1**
Image	0.9	0.7	0.8	0.5	**1**	0.2

The bold values are the extremes (zeros and ones)

Security; and Service level monitoring & management.[14] The relative importance is given by the order, following the second column of Table 11.4:

Scores

Scores in SMART can be used to convert performances (subjective or objective) to a zero-one scale, where zero represents the worst acceptable performance level in the mind of the decision maker, and one represents the ideal, or possibly the best performance desired. Note that these ratings are subjective, a function of individual preference. Scores for the criteria given in the value analysis example could be as in Table 11.6:

The best imaginable customer service level would be provided by the customizing the Australian vendor option. The South Korean ASP option is considered suspect on this factor, but not the worst imaginable. The Australian vendor system without customization is expected to be the most reliable, while the South Korean ASP options the worst. The SAP option is rated the easiest to integrate. The South Korean ASP and best-of-breed systems are rated low on this factor, but not the worst imaginable. Costs reflect Table 11.4, converting dollar estimates into value scores on the 0–1 scale. The South Korean ASP option has the best imaginable cost. The Australian vendor system without customization is rated as the best possible with respect to security issues, while the South Korean ASP is rated the worst possible. Service level ratings are high for the SAP system and the ASP, while the best-of-breed system is rated low on this factor. The highest image score is for the best-of-breed system, and the lowest for the South Korean ASP option.

Table 11.7 Worst and best measures by criteria

Criteria	Worst measure	Best measure
Customer service	0.3—South Korean ASP	1—Australian vendor
Reliability, Availability, Scalability	0—South Korean ASP	1—Australian vendor customized
Integration	0.3—Best-of-Breed & South Korean ASP	1—SAP
Cost	0.2—Best-of-breed	1—ASP
Security	0—South Korean ASP	1—Australian vendor
Service level	0.2—Best-of-Breed	1—SAP & ASP
Image	0.2—South Korean ASP	1—Best-of-Breed

Table 11.8 Weight estimation from perspective of most important criterion

Criteria	Worst measure	Best measure	Assigned value
1-Customer service	0	1	100
2-Reliability, Availability, Scalability	0	1	80
3-Integration	0	1	50
4-Cost	0	1	20
5-Security	0	1	10
6-Service level	0	1	5
7-Image	0	1	3

Weights

The next phase of the analysis ties these ratings together into an overall value function by obtaining the relative weight of each criterion. In order to give the decision maker a reference about what exactly is being compared, the relative range between best and worst on each scale for each criterion should be explained. There are many methods to determine these weights. In SMART, the process begins with rank-ordering the four criteria. A possible ranking for a specific decision maker might be as given in Table 11.7.

Swing weighting could be used to identify weights. Here, the scoring was used to reflect 1 as the best possible and 0 as the worst imaginable. Thus the relative rank ordering reflects a common scale, and can be used directly in the order given. To obtain relative criterion weights, the first step is to rank-order criteria by importance. Two estimates of weights can be obtained. The first assigns the least important criterion ten points, and assesses the relative importance of each of the other criteria on that basis. This process (including rank-ordering and assigning relative values based upon moving from worst measure to best measure based on most important criterion) is demonstrated in Table 11.8.

The total of the assigned values is 268. One estimate of relative weights is obtained by dividing each assigned value by 268. Before we do that, we obtain a second estimate from the perspective of the least important criterion, which is assigned a value of 10 as in Table 11.9.

Table 11.9 Weight estimation from perspective of least important criterion

Criteria	Worst measure	Best measure	Assigned value
7-Image	0	1	10
6-Service level	0	1	20
5-Security	0	1	30
4-Cost	0	1	60
3-Integration	0	1	150
2-Reliability, Availability, Scalability	0	1	250
1-Customer service	0	1	300

Table 11.10 Criterion weight development

Criteria	Based on best		Based on worst		Compromise
1-Customer service	100/268	0.373	300/820	0.366	0.37
2-RAS	80/268	0.299	250/820	0.305	0.30
3-Integration	50/268	0.187	150/820	0.183	0.19
4-Cost	20/268	0.075	60/820	0.073	0.07
5-Security	10/268	0.037	30/820	0.037	0.04
6-Service level	5/268	0.019	20/820	0.024	0.02
7-Image	3/268	0.011	10/820	0.012	0.01

These add up to 820. The two weight estimates are now as shown in Table 11.10.

The last criterion can be used to make sure that the sum of compromise weights adds up to 1.00.

Value Score

The next step of the SMART method is to obtain value scores for each alternative by multiplying each score on each criterion for an alternative by that criterion's weight, and adding these products by alternative. Table 11.11 shows this calculation.

In this example, the ASP turned out to be quite unattractive, even though it had the best cost and the best service level. The cost advantage was outweighed by this option's poor ratings on customer service levels expected, reliability, availability, and scalability, and security, two of which were the highest rated criteria. The value score indicates that the Australian vendor customized system would be best, followed by the SAP system and the non-customized Australian vendor system. The final ranking results reveal that adopting new technology such as ASP sometimes includes great potential risk. Multiple Criteria analysis helps focus on the tradeoffs of these potential risks.

Table 11.11 Value score calculation

Criteria	Wgt	Australian vendor	Australian vendor customized	SAP	Chinese vendor	Best-of-B	South Korean ASP
Customer service	0.37	× 0.6 = 0.222	× 1.0 = 0.370	× 0.9 = 0.333	× 0.5 = 0.185	× 0.7 = 0.259	× 0.3 = 0.111
Reliability, Availability, Scalability	0.30	× 1.0 = 0.300	× 0.8 = 0.240	× 0.9 = 0.270	× 0.5 = 0.150	× 0.4 = 0.120	× 0 = 0.000
Integration	0.19	× 0.8 = 0.152	× 0.9 = 0.171	× 1.0 = 0.190	× 0.6 = 0.114	× 0.3 = 0.057	× 0.3 = 0.057
Cost	0.07	× 0.6 = 0.042	× 0.7 = 0.049	× 0.5 = 0.035	× 0.9 = 0.063	× 0.2 = 0.014	× 1.0 = 0.070
Security	0.04	× 1.0 = 0.040	× 0.9 = 0.036	× 0.7 = 0.028	× 0.8 = 0.032	× 0.6 = 0.024	× 0 = 0.000
Service level	0.02	× 0.8 = 0.016	× 0.7 = 0.014	× 0.1 = 0.002	× 0.6 = 0.012	× 0.2 = 0.004	× 1.0 = 0.020
Image	0.01	× 0.9 = 0.009	× 0.7 = 0.007	× 0.8 = 0.008	× 0.5 = 0.005	× 1.0 = 0.010	× 0.2 = 0.002
Totals		0.781	0.887	0.866	0.561	0.488	0.260

Conclusion

Information systems security is critically important to organizations, private and public. We need the Internet to contact the world, and have benefited personally and economically from using the Web. But there have been many risks that have been identified in the open Internet environment.

A number of frameworks have been proposed. Some appear in the form of standards, such as from the International Standards Organization. That set of standards provides guidance in the macro-management of information systems security. Frameworks can provide guidance in developing processes to attain IS security, to include a Security Process Cycle and a list of best practices.

Supply chains are an especially important economic use of the Internet, and involve a special set of risks. While there are many inherent risks in electronic data interchange (needed to efficiently manage supply chains), methods have been developed to make this a secure activity in well-managed supply chains.

One way that many organizations deal with information systems is to outsource, hiring experts with strong software to do their information processing. This can be a very cost-effective means, especially for those organizations who feel that their core competencies do not include information technology (or at least all aspects of IT).

To more thoroughly evaluate information systems security, we suggest value analysis, implemented through SMART. Value analysis provides a valuable means of identifying factors of general importance. Each particular decision would be able to filter this rather long list down to those issues of importance in a particular context. Here we suggest value analysis as a means to focus on the impact of information systems security factors on alternative forms of enterprise information systems. We then demonstrated how the process, combined with SMART analysis, can be used to identify the relative importance of factors, and provide a framework to more thoroughly analyze tradeoffs among alternatives.

Notes

1. Webb, J., Ahmad, A., Maynard, S.B. and Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security* 44, 1–15.
2. Tracy, R.P. (2007). IT security management and business process automation: Challenges, approaches, and rewards, *Information Systems Security* 16, 114–122.
3. Porter, D. (2008). Business resilience, *RMA Journal* 90:6, 60–64.
4. Mijnhardt, F., Baars, T. and Spruit, M. (2016). Organizational characteristics influencing SME information security maturity. *Journal of Computer Information Systems* 56(2), 106–115.
5. Gikas, C. (2010). A general comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS standards. *Information Security Journal: A Global Perspective* 19(3), 132–141.
6. Da Veiga, A. and Eloff, J.H.P. (2007). An information security governance framework, *Information Systems Management* 24, 361–372.

7. Tudor, J.K. (2000). *Information Security Architecture: An Integrated Approach to Security in an Organization*. Boca Raton, FL: Auerbach.
8. McCarthy, M.P. and Campbell, S. (2001). *Security Transformation*. New York: McGraw-Hill.
9. Tracy (2007), op cit.
10. Ibid.
11. VandePutte, D. and Verhelst, M. (2013). Cyber crime: Can a standard risk analysis help in the challenges facing business continuity managers? *Journal of Business Continuity & Emergency Planning* 7(2), 126–137.
12. Keller, S., Powell, A., Horstmann, B., Predmore, C. and Crawford, M. (2005). Information security threats and practices in small businesses, *Information Systems Management* 22, 7–19.
13. Faisal, M.N., Banwet, D.K. and Shankar, R. (2007). Information risks management in supply chains: An assessment and mitigation framework, *Journal of Enterprise Information Management* 20:6, 677–699.
14. Cigolini, R. and Rossi, T. (2006). A note on supply risk and inventory outsourcing, *Production Planning and Control* 17:4, 424–437.
15. Smith, G.E., Watson, K.J., Baker, W.H. and Pokorski, J.A. II (2007). A critical balance: Collaboration and security in the IT-enabled supply chain, *International Journal of Production Research* 45:11, 2595–2613.
16. Dhillon, G. and Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations, *Information Systems Journal* 16, 293–314.
17. Olson, D.L. (2004). *Managerial Issues in Enterprise Resource Planning Systems*. New York: McGraw-Hill/Irwin.
18. Olson, D.L. (2007). Evaluation of ERP outsourcing. *Computers & Operations Research* 34, 3715–3724.
19. Olson, D.L. (1996). *Decision Aids for Selection Problems*. New York: Springer.
20. Van Everdingen, Y., van Hellegersberg, J. and Waarts, E. (2000). ERP adoption by European midsize companies. *Communications of the ACM* 43(4), 27–31.
21. Ekanayaka, Y., Currie, W.L. and Seltsikas, P. (2003). Evaluating application service providers. *Benchmarking: An International Journal* 10(4), 343–354.
22. Olson, D.L. (2007). Evaluation of ERP outsourcing. *Computers & Operations Research* 34, 3715–3724.