Taylor & Francis
Taylor & Francis Group

Information Security Journal: A Global Perspective

ISSN: 1939-3555 (Print) 1939-3547 (Online) Journal homepage: http://www.tandfonline.com/loi/uiss20

Potential Problems with Information Security Risk Assessments

Richard G. Taylor

To cite this article: Richard G. Taylor (2015): Potential Problems with Information Security Risk Assessments, Information Security Journal: A Global Perspective, DOI: 10.1080/19393555.2015.1092620

To link to this article: http://dx.doi.org/10.1080/19393555.2015.1092620

Information Security Journal: A Global Perspective, 00:1–8, 2015

ISSN: 1939-3555 print / 1939-3547 online
DOI: 10.1080/19393555.2015.1092620

Taylor & Francis
Taylor & Francis Group

Potential Problems with Information Security Risk Assessments

Richard G. Taylor
Jesse H. Hones School of Business, Department of Business Administration, Texas Southern University, Houston, Texas, USA

ABSTRACT To protect the information assets of any organization, management must rely on accurate information security risk management. Management must access the risk to the organizations assets then develop information security strategies to reduce the risks. This assessment is difficult because of rapidly changing technology and new threats that are frequently being discovered. Research to address methods associated with information security risk management includes quantitative and qualitative methods. More comprehensive approaches combine both the quantitative and qualitative methods. This paper argues that current methods of information security assessment are flawed because management decisions regarding information security are often based on heuristics and optimistic perceptions.

KEYWORDS information, risk, security assessment, vulnerabilites

Information security risk assessment involves identifying potential threats to organizational information which could result in information security incidents. An information security threat is considered any actions that could result in an undesirable effect to organizational information (Farahmand, Navathe, Sharp, & Enslow, 2005). The source of these threats can be natural or environmental (e.g., floods, earthquakes, hurricanes, tornados), human (intentional or unintentional actions), and/or technical (e.g., viruses, worms, denial of service [DoS] attacks, hacker attacks). These threats may come from outside an organization or from within (Maasberg & Beebe, 2014; Taylor, 2008). When a threat results in a breach in an organization's security, whether it results in loss or not, it is considered a security incident (Cashell, Jackson, Jickling, & Webel, 2004).

An absence of security incidents is not a sure sign of good security. There may be incidents that go unnoticed, or organizations may just be lucky. Being unaware of security incidents or relying on luck to protect organizational information are signs of poor information security management.

Although it is impossible to eliminate all information security risks (Cavusoglu, Mishra, & Raghunathan, 2005) several studies show that security countermeasures can be used to reduce information security risks (Madnick, 1978; Martin, 1973; Mejias, 2014; Straub, 1990; Straub & Nance, 1990; Straub & Welke, 1998).

Address correspondence to Richard G. Taylor, Jesse H. Hones School of Business, Department of Business Administration, Texas Southern University, 3100 Cleburne Street, Houston, TX 77004.
E-mail: taylorrg@tsu.edu

SECURITY COUNTERMEASURES

Goodhue and Straub (1991) identified four components of security countermeasures: deterrence, prevention, detection, and remedies.

Deterrent countermeasures are typically nontechnology-based methods aimed at deterring information security incidents. Deterrent countermeasures include security policies and security awareness training. In contrast, the purpose of preventative security countermeasures is to actually prevent the information security incident from occurring. Preventative countermeasures include firewalls, anti-virus software, intrusion detection systems, encryption for transmitted data, public key infrastructure, intrusion prevention systems, and access control. Detection countermeasures involve monitoring activities such as security cameras, email logs, firewall logs, intrusion detection reports, and audits to identify information security vulnerabilities. Finally, remedies consist of actions taken after the discovery of a security incident. Remedy countermeasures include correcting security vulnerabilities, updating policies and procedures, and punishing those responsible for the incidents.

To reduce an organization's information security risk, security countermeasures should be instituted. It is ultimately management's responsibility to determine the types of countermeasures to institute to minimize the information security risks within their organizations. However, instituting security countermeasures requires a high degree of managerial vigilance (Goodhue & Straub, 1991).

The mere presence of security countermeasures does not ensure a reduction in information security risk. Even with countermeasures, chances of a security incident still remain high (Farahmand et al., 2005). Information security policies may exist, but will be ineffective if the policies are not read and understood by employees (Taylor, 2006; Taylor & Brice, 2012). Access controls may be instituted, requiring passwords to access computer-based systems. However, if weak passwords or repeated passwords are allowed, then access control may prove to be an ineffective method for protecting computer-based systems (Mattord, Levy, & Furnell, 2014; Zviran, 1999).

The same applies to other security countermeasures, including firewalls, virus protections software, and so forth. These countermeasures may be effective for protecting organizational information; however, they are installed by humans and configured by humans, which adds an error component to their effectiveness (Dhillon & Backhouse, 2000). Firewalls and intrusion detection systems must be properly interfaced with the other computer-based system components and the controls must be configured to allow the proper balance between security and operations (Cavusoglu et al., 2005). The same applies to virus-protection software. New viruses are created almost daily (HFC, 2003). If the virus definitions in the virus-protection software are not continuously updated, then the organization will be left unprotected from these new strains of viruses. It becomes important to not only observe the presence of security countermeasures, but to also investigate their effectiveness.

> Responsible management must ask not only which dangers are the worst but also which are the most amenable to treatment. A safety measure that is reasonable in a cost-benefit sense may not seem reasonable in a cost-effectiveness sense. That is, if our safety dollars are limited, finding that the benefits of a particular safety measure outweigh its costs does not preclude the possibility that even greater benefits could be reaped with a like expenditure elsewhere. (Fischhoff, Slovic, & Lichtenstein, 1979, p. 34)

To address this problem, management must decide which information security threats are the most likely to occur and which security countermeasures will provide the greatest reduction in information security risk. Past research has attempted to determine the proper amount to invest in security countermeasures (Anderson, 2001; Buzzard, 1999; Finne, 1998; Gordon & Loeb, 2002; Hoo, 2000; Jones, 1997; Meadows, 2001; Millen, 1992); however, no consensus has been reached. Ultimately, instituting security countermeasures is a management decision influenced by many factors. Resources are limited; therefore, decision makers must decide which threats pose the greatest risks to their organizations and then institute security countermeasures to combat those threats (Norman, 2010). The lack of sufficient security budgets is often an obstacle to achieving the desired level of information security protections (Johnson, Goetz, & Pfleeger, 2009; Yue, Çakanyıldırım, Ryu, & Liu, 2007). Given the budgetary constraints, it is important that organizations carefully consider information security risk management before security decisions are made. Information security risk management must identify the potential threats, prioritize the threats, assess the risks posed by those threats, and select the appropriate countermeasures to reduce the risks (Yue et al., 2007).

However, security decisions may not be rationally based, leaving organizations open to information security threats (Goodhue & Straub, 1991).

DECISION MAKING

Decision research has been conducted that is both normative and descriptive in nature (Kahneman & Tversky, 1984). "The normative analysis is concerned with the nature of rationality and the logic of decision making. The descriptive analysis, in contrast, is concerned with people's beliefs and preferences as they are, not as they should be" (Kahneman & Tversky, 1984, p. 341). The process of risk analysis generates information that will be used in decision making. How the information is used is determined by who receives the information, the institutional objectives, and the environment in question (Greenberg et al., 2012). A decision-maker's choice of a specific option is based on the difference between the option's advantages and disadvantages. Those options whose advantages exceed their disadvantages are considered optimal (Kahneman & Tversky, 1984). These decisions should be conducted in a calculated and probabilistic manner, allowing the decision maker to select the option that maximizes utility. "Solutions to the problem of coping with hazards have typically been justified by a computation of benefits and costs that assume the people involved will behave in what the policy maker considers to be an economically rational way" (Slovic, Kunreuther, & White, 1974).

Expected utility theory (EUT) is accepted as a normative model for making rational choices under conditions of risks or uncertainty (Kahneman & Tversky, 1979). "Risk is most commonly conceived as reflecting variation in the distribution of possible outcomes, their likelihoods, and their subjective values" (March & Shapira, 1987, p. 1404). Risk analysis is used by decision makers to determine security countermeasures that should be instituted in their organization to address information security threats (Feng, Wang, & Li, 2014). One method for measuring information security risks is annualized loss expectancy (ALE), which uses the foundations of expected utility theory (FIPSPUB, 1974). Information security risks are measured by the potential loss an organization could expect from an information security incident. ALE is calculated as follows:

$$\mathbf{ALE} = \mathbf{P}_i \times \mathbf{C}_i$$

P_i represents the probability of threat i, and C_i represents the potential loss from threat i.

P_i is a number between zero (a threat expected not to occur) and one (a threat the will definitely occur). ALE has been used by organizations to rank different information security threats. Threats with the greatest ALE are considered to pose the greatest risk. ALE can also be used to determine the net benefit of instituting security countermeasures to combat specific threats. Should organizations invest in a security countermeasures as long as the cost of the countermeasures is less than the ALE? This becomes a question similar to the one organizations face when purchasing insurance. ALE assumes that the probability of an information security threat is known and that the total potential loss can be determined. However, research has shown that both of these variables resist quantification (Cashell et al., 2004). Attempts to calculate a value for ALE run afoul of "the unrealistic and time-wasting assumption of numerically precise information" (Ekenberg, Oberoi, & Orci, 1995 p. 715). ALE considered the probability of the threat and the potential loss from a threat; however ALE failed to consider the vulnerability an organization has to the threat in question.

Gordon and Loeb (2002) created an economic model to determine the expected loss (EL) from an information security threat, including vulnerability (V) as a variable:

$$\mathbf{EL} = \mathbf{P}_i \times \mathbf{V}_i \times \mathbf{C}_i$$

EL represents the expected loss resulting from an information security incident. P_i is the probability of threat i occurring, C_i is the potential loss from threat i, and V_i is the vulnerability of the organization to threat i. Gordon and Loeb point out that P_i and C_i are factors that cannot be controlled by the organization. For example, an organization has no control over the number of viruses or the propensity of a thief to steal information. Costs due to an information security incident are also assumed to be uncontrollable. However, the organization does have control over security countermeasures instituted to protect the organization from threats. Therefore, V_i is a function of the threat and the organization's preparation to deal with the threat. "For any positive threat (P_i>0), the expected loss increases with the vulnerability" (Gordon & Loeb, 2002, p. 442). Security countermeasures are instituted to decrease an organization's vulnerability to an information security threat, lowering V_i, and thus reducing the expected loss. Gordon and Loeb (2002) refer to this as the 'security breach probability function' (S):

$$\mathbf{S}(\mathbf{Z}, \mathbf{V})$$

Z represents the investment in security countermeasures to protect the organizations and V represents the vulnerability. An investment Z is made to lower the probability of

an information security incident. Therefore, the security breach probability function (S) denotes the organization's vulnerability to an information security incident after a specified investment has been made to prevent the information security threat (Gordon & Loeb, 2002).

The problems with these methods (ALE and EL) are that they require the decision maker to determine 1) the potential loss due to a threat, 2) the probability of a threat occurring, and 3) the vulnerability of the organization to the threat. If not accurate, each of these determinations can lead to misperceptions of risks.

Potential Costs/Losses Due to Information Security Incidents

For organizations to understand the cost/benefit analysis of instituting security countermeasures, they must fully understand both the tangible and intangible costs associated with an information security threat (Farahmand et al., 2005). Research has attempted to quantify these costs; however, the calculation methods are based mostly on subjective estimations of both probability of the threat and expected cost of the loss (Farahmand et al., 2005; Gordon & Loeb, 2002). One reason is the difficulty involved with identifying possible losses from different types of information security threats, both tangible and intangible.

> A complete list of things that can go wrong with information systems is impossible to create. People have tried to create comprehensive lists, and in some cases have produced encyclopedic volumes on the subject, but there are potentially infinite number of different problems that can be encountered, so any list can only serve a limited purpose. (Farahmand et al., 2005, p. 213)

When people judge risks, they tend to rely on their own estimates rather than actual data (Slovic, Fischhoff, & Lichtenstein, 1979). This may also be the case with judging the potential loss from an information security incident. Do managers actually calculate the potential losses, both tangible and intangible, for a specific information systems security threat, or do they use estimates? If estimates are used, how accurate are these estimates?

It is crucial for organizations of all sizes to be able to determine the potential loss from an information security incident (Farahmand et al., 2005). However, even if all information security incidents could be quantified and their probability of occurrence assessed, it is still difficult to put a price tag on the potential losses (Fischhoff et al., 1979). Research has shown that an organization's stock price can be negatively affected due to an information security incident (Das, Mukhopadhyay, & Anand, 2012; Cashell et al., 2004; Chen, Bose, Leung, & Guo, 2011). Tangible losses, such as damage to physical equipment or property, may be easier to quantify. However, it should be noted that identical information security incidents can result in different amount of losses for different organizations, even within the same industry type (Farahmand et al., 2005). Beyond the immediate financial costs and losses, organizations must also consider the intangible impacts, which most often present themselves as hidden costs that are difficult to quantify (Table 1).

TABLE 1 Intangible costs of an ISS incident (Farahmand et al., 2005)

Intangible Costs of an ISS Incident
The brand image, public reputation and goodwill in the marketplace
The financial value of business transactions
Public and customer confidence in the accuracy of business transactions
Public and customer confidence in the fraud-resistance of business transactions
The ability to maintain revenue cash flow in a timely manner
The ability to resolve disputes beyond reasonable doubt
The ability to meet the requirements of regulators

The potential economic impact of an information security incident must ultimately be speculative (Cashell et al., 2004). The inability to accurately quantify potential losses from information security incidents becomes a problem for decision makers (Farahmand, Navathe, Sharp, & Enslow, 2003).

Probabilities of Information Security Incidents

Accessing the probability of an information security incident is a different task. For some threats, such as the frequency of automobile accidents, there is extensive statistical data available; however, other threats are less understood because of a lack of data (Slovic et al., 1979). Statistical data about information security incidents and threats are not as available as other data. This is attributable to several reasons: 1) the historical data to soundly base future projections of risks is still limited, 2) organizations do not report information security incidents for fear of negative ramifications, and 3) organizations may be unaware they have been the victim of an information security incident (Kesan, Majuca, & Yurcik, 2004). A World Bank Study found that "the existing base of information

that supports projections about the extent of the . . . security problem is substantially flawed" (Glaessner, Kellerman, & McNevin, 2002, p. 16).

Even insurance companies recognize the difficulty of determining information security risk probabilities. Cyber insurance to protect organizations from losses due to information security incidents shows slow growth, hindered by the lack of empirical data needed to construct actuarial tables. Insurers are not able to determine probabilities with the same degree of certainty they can in traditional insurance lines (Cashell et al., 2004). It is easy for an insurance company to determine the probability of someone dying from an automobile accident or airplane crash; however, it is much more difficult to determine the probability of a financial loss due to a hacker intrusion or the loss of a backup tape.

Vulnerabilities to Information Security Incidents

Even when statistical data does exist, human judgment still plays a role in interpreting the data and applying the meaning to their specific situation (Slovic et al., 1979). A commonly used methods for assessing the probability of information security incidents and the vulnerability of an organization to an information security threat is a subjective analysis of costs and probabilities based on existing security countermeasures (Farahmand et al., 2003).

The National Institute of Standards and Technology (NIST) and Federal Emergency Management Agency (FEMA) have developed subjective methods to determine organizational vulnerability of information security threats. These methods attempt to assign a semi-quantitative value based on subjective judgments.

In the NIST model, the likelihood of an information security threat is assigned a probability value based on the organization's preparedness to deal with the threat. The next step involves assigning a value to the level of impact the threat would have on the organization, determined by the potential loss. Based on those values, an overall risk score is calculated (Table 2). Information security threats with the highest risk scores are those that are recommended to receive the highest priority when implementing security countermeasures.

This method, though widely used to determine information security risks, is based on the decision-maker's perceptions of the likelihood and potential impact of an information security threat. The model also fails to consider the costs of security countermeasures and past history of the effectiveness of security countermeasures that can be instituted to deter or prevent the information security threat.

HEURISTICS AND PERCEPTIONS

The theory of bounded rationality presents an alternative to expected utility theory. Bounded rationality asserts that "the cognitive limitations of the decision-maker force him to construct a simplified model of the world to deal with it" (Slovic et al., 1974, p. 5). Instead of maximizing utility, bounded rationality focuses on "satisficing," which refers to attempting to attain a satisfactory, though not maximal, outcome. Bounded rationality theory has been used to investigate management decisions based on risk perception (Slovic, 1987; Starr, 1969). Rational decision making is not always used "when judging probabilities, making predictions, or attempting to cope with probabilistic tasks" (Slovic, 1987, p. 281). Instead, managers tend to use judgmental heuristics which may be valid in certain circumstances, but in others they can lead to biases that are "large, persistent and serious in their implications for decision making" (Slovic, Fischhoff, & Lichtenstein, 1976, p. 36). Therefore, managers make decisions without the availability of all the potentially necessary information.

When decision makers evaluate risks, they do not always have supporting statistical evidence at hand. They typically

TABLE 2 Assessment scale—level of risk (NIST, 2012)

	Level of Impact				
Likelihood of Threat	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Very High (96–100), High (80–95), Moderate (21–79), Low (5–20), Very Low (0–4).

rely on inferential-based understandings of the risks (Slovic et al., 1979). These inferences are dictated by a set of judgmental heuristics to simplify the task of decision making (Tversky & Kahneman, 1974). Heuristics are often based on past experiences and can lead to appropriate decisions but "they can lead to large and persistent biases with serious implications for risk assessment" (Slovic et al., 1979, p. 15). These faulty risk perceptions may increase with technology-based decisions because of managements' lack of understanding of technology or risks may by overlooked because of the perceived benefits of the technology. Three heuristics have been identified that affect the assessment of probabilities: 1) representativeness, 2) availability, and 3) anchoring and adjustment (Tversky & Kahneman, 1974).

Representativeness

Representativeness refers to similarities a person or event has to another person or event (Tversky & Kahneman, 1974). For example, if an information security incident has not occurred in the organization's industry then decision makers may not properly access the probability of a similar incident occurring in their organization. In December 2013, Target Stores became the victim of hackers who were able to breach their system and steal customer information. Prior to the event no recent publicized attacks on retail store were reported. Therefore information security was not necessarily at the forefront of Target's priorities.

Availability

Availability is based on the ability to recall an event (Tversky & Kahneman, 1974). The probability of an event, such as an information security incident, may be influenced by a recent event personally experienced or by an event that was recently publicized (Kasperson et al., 1988). If a manager hears a news report about a security breach, he or she may be more inclined to focus on security countermeasures to prevent such an incident from occurring at their organization. Using the above Target example, once the data breach was publicized, it would be expected that other managers in the retail industry would be more likely to reevaluate their information security strategy to prevent a similar event from happening to their organization. It should be noted that some organizations have the "it won't happen to me" ideology. Shortly after the security breach at Target, Neiman Marcus and Nordstrom's stores were attacked in the same manner, resulting in the loss of customer information.

Anchoring and Adjustment

Anchoring and adjustment involves making probability estimates by starting at an initial value, then adjusting the probability from the starting point (Tversky & Kahneman, 1974). Decisions that are made quickly, based on emotions and intuition, can influence the anchor used in initial risk evaluations (Greenberg et al., 2012). For example, a manager may perceive that the probability of a hacker attack is 75%; however, he or she may perceive that with security countermeasures in place, the organization's vulnerability will be reduced by 50%, resulting in an overall risk of 25%. However, if the starting value of 75% is incorrect, then the final value will also be incorrect, thus leaving the organization more exposed than perceived. In the situations like Target and Neiman Marcus, the organizations' security assessments were flawed, miscalculating the probability of the attacks or the effectiveness of their security countermeasures, or both.

Decision makers tend to feel confident about their heuristic-based decisions. "Such overconfidence is dangerous. It indicates that we often do not realize how little we know and how much additional information we need about the various problems and risks we face" (Slovic et al., 1979, p. 17). The heuristic-based decisions are largely based on the decision-makers perceptions (Kahneman, 1994). If an organization were to experience a single dramatic information security incident, a significant shift in their risk perception could occur (Cashell et al., 2004). Surely this was the case for Target, Nordstrom's, and Neiman Marcus. After their highly publicized losses, managements' risk perceptions would be changed, resulting in a more thorough information security risk assessment.

CONCLUSION

Past methods, such as ALE and the Gordon and Loeb (2002) model, attempted to use a utility-based approach to determine information security risk. Each of these methods are based on the accurate determination of the probability of an information security incident occurring and of the potential loss from the incident. The Gordon and Loeb (2002) model includes the vulnerability factor, representing the perceived probability of a threat occurring with specified security countermeasures in place. However, Gordon and Loeb make the assumption that an organization's vulnerability to a threat is based solely on financial investments in security countermeasures. Research has shown that the mere presence of security

countermeasures does not insure adequate information security protection (Farahmand et al., 2005). Security countermeasures must be properly managed to be effective. Although research has shown that a utility-based approach can be effective when making decisions regarding risks, this paper argues that information security probabilities are often determined by perceptions and heuristics which can ultimately lead to inaccurate risks determinations when these methods are used. Therefore, careful consideration should be taken when using these, or other models, to determine an organizational security risks.

This paper suggests that one flaw that will continually plague the efforts for accurate risk assessment is the necessity to rely on management perceptions, which when based on heuristics instead of facts, can lead to flawed organizational strategy and increased industry threats. Organizational theorists suggest that decisions made in the fog of misleading perceptions tend to lead to flawed organizational strategy (Bourgeois, 1985; Boyd, Dess, & Rasheed, 1993), and can result in operational risks and industry threats (Barr, Stimpert, & Huff, 1992; Starbuck, 1992).

There is still no agreed upon method to measure information security risks. While many methods have been proposed, and are currently being used, researchers have noted that flaws still exist that prevent accurate information security risk assessment. Quantitative methods of risk analysis may not include all necessary variables, while qualitative methods tend to yield inconsistent results (Karabacak & Sogukpinar, 2005).

Information security risk management is an imprecise science. Risk management requires an accurate security assessment, which can ultimately be a difficult process because of many practical uncertainties. Decisions are often made without the required information, and instead based on management assumptions. Failing to properly identify and estimate the necessary variables can ultimately have critical negative impacts on an organization.

REFERENCES

Anderson, R. (2001). *Why information security is hard–An economic perspective*. 17th Annual Computer Security Applications Conference (ACSAC), New Orleans, LA.

Barr, P., Stimpert, J. L., & Huff, A. S. (1992). Cognitive change, strategic action and organizational renewal. *Strategic Management Journal*, *13*, 15–36. doi:10.1002/(ISSN)1097-0266

Bourgeois, L. J. (1985). Strategic goals, perceived uncertainty, and economic performance in volatile environments. *Academy of Management Journal*, *28*, 548–573. doi:10.2307/256113

Boyd, B. H., Dess, G. G., & Rasheed, A. M. (1993). Divergence between archival and perceptual measures of the environment: Causes and consequences. *Academy of Management Review*, *18*, 204–226.

Buzzard, K. (1999). Computer security — What should you spend your money on? *Computers & Security*, *18*(4), 322–334. doi:10.1016/S0167-4048(99)80078-9

Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). *The economic impact of cyber attacks - CRS report for Congress*. G. A. F. Division, The Library of Congress, 1–41.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2005). The value of intrusion detection systems in information technology security architecture. *Information Systems Research*, *16*(1), 28–46. doi:10.1287/isre.1050.0041

Chen, X., Bose, I., Leung, A., & Guo, C. (2011). Assessing the severity of phishing attacks: A hybrid data mining approach. *Decision Support Systems*, *50*(4), 662–672. doi:10.1016/j.dss.2010.08.020

Das, S., Mukhopadhyay, A., & Anand, M. (2012). Stock market response to information security breach: A study using firm and attack characteristics. *Journal of Information Privacy and Security*, *8*(4), 27–55. doi:10.1080/15536548.2012.10845665

Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, *43*(7), 125–128. doi:10.1145/341852.341877

Ekenberg, L., Oberoi, S., & Orci, I. (1995). A cost model for managing information security hazards. *Computers & Security*, *14*, 707–717. doi:10.1016/0167-4048(95)00021-6

Farahmand, F., Navathe, S., Sharp, G. P., & Enslow, P. H. (2003). *Managing vulnerabilities of information systems to security incidents*. ACM International Conference on Electronic Commerce, Pittsburgh, PA.

Farahmand, F., Navathe, S. B., Sharp, G. P., & Enslow, P. H. (2005). A management perspective on risk of security threats to information systems. *Information Technology and Management*, *6*, 203–225. doi:10.1007/s10799-005-5880-5

Feng, N., Wang, H. J., & Li, M. (2014). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. *Information Sciences*, *256*, 57–73. doi:10.1016/j.ins.2013.02.036

Finne, T. (1998). A conceptual framework for information security management. *Computers & Security*, *17*(4), 303–307. doi:10.1016/S0167-4048(98)80010-2

FIPSPUB. (1974). *National Institute of Standards and Technology, Guidelines for Automatic Data Processing Physical Security and Risk Management*, June 1974.

Fischhoff, B., Slovic, P., & Lichtenstein, S. (1979). Weighing the risks: Risks: Benefits which risks are acceptable? *Environment: Science and Policy for Sustainable Development*, *21*(4), 17–38. doi:10.1080/00139157.1979.9929722

Glaessner, T., Kellerman, T., & McNevin, V. (2002). *Electronic security: Risk mitigation in financial transactions*. World Bank: 16.

Goodhue, D., & Straub, D. (1991). Security concerns of system users. A study of perceptions of the adequacy of security. *Information & Management*, *20*, 13–27. doi:10.1016/0378-7206(91)90024-V

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, *5*(4), 438–457. doi:10.1145/581271.581274

Greenberg, M., Hass, C., Cox, A. L., McComas, K., & North, W. (2012). Ten most important accomplishments in risk analysis, 1980–2010. *Risk Analysis*, *32*(5), 771–781. doi:10.1111/j.1539-6924.2012.01817.x

HFC. (2003). *The alarming state of security management practices among organizations worldwide. Security management index*. Retrieved from http://www.humanfirewall.org

Hoo, K. (2000). *How much is enough? A risk-management approach to computer security*. Consortium for Research on Information Security Policy (CRISP), Stanford, CA: Stanford University.

Johnson, M. E., Goetz, E., & Pfleeger, S. L. (2009). Security through information risk management. *IEEE Security & Privacy Magazine*, *7*(3), 45–52. doi:10.1109/MSP.2009.77

Jones, A. (1997). Penetration testing and system audit. *Computer Security*, *19*, 595–602. doi:10.1016/S0167-4048(97)80796-1

Kahneman, D. (1994). New challenges to the rationality assumption. *Journal of Institutional and Theoretical Economics*, *150*, 18–36.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica*, *47*, 263–291. doi:10.2307/1914185
Kahneman, D., & Tversky, A. (1984). Choices, values, and frames. *American Psychologist*, *39*(4), 341–350. doi:10.1037/0003-066X.39.4.341
Karabacak, B., & Sogukpinar, I. (2005). ISRAM: Information security risk analysis method. *Computers & Security*, *24*(2), 147–159. doi:10.1016/j.cose.2004.07.004
Kasperson, R. E., Renn, O., Slovic, P., Brown, H., Emel, J., Goble, R. . . . Ratick, S. (1988). The social amplification of risk: A conceptual framework. *Risk Analysis*, *8*(2), 177–187. doi:10.1111/risk.1988.8.issue-2
Kesan, J., Majuca, R., & Yurcik, W. (2004). *The economic case for cyberinsurance. Securing privacy in the internet age symposium*, Stanford, CA: Stanford University.
Maasberg, M., & Beebe, N. L. (2014). The enemy within the insider: Detecting the insider threat through addiction theory. *Journal of Information Privacy and Security*, *10*(2), 59–70. doi:10.1080/15536548.2014.924807
Madnick, S. (1978). Management policies and procedures needed for effective computer security. *Sloan Management Review*, *20*(1), 61–74.
March, J. G., & Shapira, Z. (1987). Managerial perspectives on risk and risk taking. *Management Science*, *33*(11), 1404–1418. doi:10.1287/mnsc.33.11.1404
Martin, J. (1973). *Security, accuracy, and privacy in computer systems*. Englewood Cliffs, NJ: Prentice-Hall.
Mattord, H. J., Levy, Y., & Furnell, S. (2014). Factors for measuring password-based authentication practices. Journal of Information Privacy and *Security*, *10*(2), 71–94.
Meadows, C. (2001). A cost-based framework for analysis of denial of service in networks. *Journal of Computer Security*, *9*(1/2), 143–164.
Mejias, R. J. (2014). A model of information security awareness for assessing information security risk for emerging technologies. *Journal of Information Privacy and Security*, *10*(4), 160–185. doi:10.1080/15536548.2014.974407
Millen, J. (1992). *A resource allocation model for denial of service*. Proceedings of the 1992 IEEE Symposium on Security and Privacy. Los Alamos, CA, IEEE Computer Society Press: 137–147.
NIST. (2011). *NIST SP 800-39, Managing information security risk: Organization, mission, and information system view*. March 2011. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf
NIST. (2012). *NIST SP 800-30 Rev. 1, Guide for conducting risk assessments*. September, 2012. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
Norman, T. L. (2010). *Risk analysis and security countermeasure selection*. Boca Raton, FL: CRC Press.
Slovic, P. (1987). Perception of risk. *Science*, *236*, 280–285. doi:10.1126/science.3563507
Slovic, P., Fischhoff, B., & Lichtenstein, S. (1976). *Cognitive processes and societal risk taking. Cognition and social behavior* (J. S. Carroll & J. W. Payne, Eds.; pp. 165–184). Potomac, MD: Erlbaum.
Slovic, P., Fischhoff, B., & Lichtenstein, S. (1979). Rating the risks. *Environment: Science and Policy for Sustainable Development*, *21*(3), 14–39. doi:10.1080/00139157.1979.9933091
Slovic, P., Kunreuther, H., & White, G. F. (1974). *Decision processes, rationality, and adjustment to natural hazards. Natural hazards: local, national, Global. G. F. White*. London: Oxford University Press.
Starbuck, W. H. (1992). Strategizing in the real world. *International Journal of Technology Management. Special Publication on Technological Foundations of Strategic Management*, *8*(1/2), 77–85.
Starr, C. (1969). Social benefit versus technological risk. *Science*, *165*, 1232–1238. doi:10.1126/science.165.3899.1232
Straub, D. (1990). Effective IS security: An empirical study. *Information Systems Research*, *1*(3), 255–276. doi:10.1287/isre.1.3.255
Straub, D., & Nance, W. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly*, *14*(1), 45–60. doi:10.2307/249307
Straub, D., & Welke, R. (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, *22*(4), 441–469. doi:10.2307/249551
Taylor, R., & Brice, J. (2012). Fact or fiction? A study of managerial perceptions applied to an analysis of organizational security risk. *Journal of Organizational Culture, Communications, and Conflict*, *16*(1), 1–23.
Taylor, R. G. (2006). *Management perception of unintentional information security risks*. Proceedings of the twenty-seventh International Conference on Information Systems, Milwaukee, WI.
Taylor, R. G. (2008). The social side of security. In I. Chen, & T. Kidd (Eds.), *Social information technology: Connecting society and cultural issues* (pp. 140–150). Hershey, PA: Idea Group.
Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science*, *185*, 1124–1131. doi:10.1126/science.185.4157.1124
Yue, W. T., Çakanyıldırım, M., Ryu, Y. U., & Liu, D. (2007). Network externalities, layered protection and IT security risk management. *Decision Support Systems*, *44*(1), 1–16. doi:10.1016/j.dss.2006.08.009
Zviran, M. (1999). Password security: An empirical study. *Journal of Management Information Systems*, *15*(4), 161–186.

BIOGRAPHY

Dr. Richard Taylor is an assistant professor at Texas Southern University in Houston, Texas. He received his PhD in Management Information Systems from the University of Houston. His research interests include the social impact of information security, employee information security behavior, and managerial information security risk assessment.