Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2015 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-13-2015

Why Cooperate? Ethical Analysis of InfoSec Vulnerability Disclosure

Mark-David McLaughlin
Cisco Systems/Bentley University

Janis Gogan
Bentley University

Why Cooperate?

Ethical Analysis of InfoSec Vulnerability Disclosure

Mark-David McLaughlin
Cisco Systems/Bentley University, Waltham MA USA

Janis L. Gogan
Bentley University, Waltham MA USA

ABSTRACT

Vendors, security consultants and information security researchers seek guidance on *if* and *when* to disclose information about specific software or hardware security vulnerabilities. We apply Kantianism to argue that vendors and third parties (InfoSec researchers, consultants, and other interested parties) have an ethical obligation to inform customers and business partners (such as channel partners or providers of complementary products and services) about specific software vulnerabilities (thus addressing *if* disclosure should occur). We apply Utilitarianism to address the question of *when* disclosure should occur. By applying these two philosophical perspectives we conclude that to maximize social welfare, vendors should release software fixes as soon as possible, and third parties should adopt a coordinated disclosure policy to avoid placing customers and business partners at unnecessary risk.

Keywords: Information Systems Security, Ethics, Vulnerability Disclosure, Kantianism, Utilitarianism

INTRODUCTION

Rarely is software released without defects. An information security (InfoSec) *vulnerability* is a specific type of software defect that enables a malicious agent to undermine the confidentiality, integrity, or availability of an IT product or service (device, database, system software, or software application). After a vulnerability is identified in an IT product, customers and business partners expect the vendor to produce a fix and inform the public about risks they will face if they do not install it. If a vendor believes no one else has discovered the vulnerability as yet, and/or that it has not yet been maliciously exploited by hackers, they may not feel moral pressure to disclose it and provide a fix. Therefore, *when* and *how* to inform customers of InfoSec vulnerabilities remains an open question. This paper addresses ethical considerations related to the disclosure of InfoSec vulnerabilities in hardware and software.

Organizations that do not disclose InfoSec vulnerabilities place their customers at risk. Because no centralized authority governs computer use, significant organizations' vulnerability disclosure policies and procedures vary, and different ethical codes have been adopted by different software and equipment vendors, consultants, end users, and researchers (Leiwo and Heikkuri 1998). Guidelines suggests that vulnerability disclosure policies should address vendor *responsibility* (ownership and accountability of issues), *morality* (acting responsibly), *trust* (instill confidence), and *ethicality* (acting in accordance with principles of right conduct) (Dhillon and Backhouse 2000). While prior studies have examined InfoSec vulnerability disclosure issues, to our knowledge, no paper has done so through the lens of ethical theories. We fill that gap by drawing on Kantianism and Utilitarianism to provide ethical guidance to the following research questions:

RQ1a: Should organizations publicly disclose InfoSec vulnerabilities in their hardware and software products and services?

RQ1b: If so, *how soon* should organizations disclose these InfoSec vulnerabilities?

RQ2a: Should third parties (customers, consultants, security researchers, etc.) who become aware of previously-undisclosed nfoSec vulnerabilities publicly disclose them?

RQ2b: If so, *how soon* should third parties disclose these InfoSec vulnerabilities?

INFOSEC VULNERABILITY DISCLOSURE: PRIOR RESEARCH

If a vendor chooses not to disclose InfoSec vulnerabilities lurking in their products, or not to fix them, customers will come to distrust them. Responsible disclosure programs aim to disclose vulnerabilities to "the appropriate people, at appropriate times, and through appropriate channels" to minimize potential negative impacts to society (Cavusoglu et al. 2005). Yet, how and when to disclose vulnerability information is not a straightforward decision. While public disclosure increases awareness of a vulnerability (giving customers and business partners an opportunity to install a fix or prepare for an attack), disclosure also increases the likelihood that malicious agents will learn about the vulnerability and attempt to exploit it. Many vendors reportedly release patches before it is socially optimal to do so (Cavusoglu and Raghunathan 2007), and simulations reveal that neither instant disclosure nor secrecy maximizes social welfare (Arora et al. 2008). We further note that disclosure of a particular vulnerability does not guarantee that all customers and partners will remediate it; some customers will not install a fix due to various circumstances. They may have been unable to receive a vendor notification when it was distributed, or may not have the expertise to perform the mitigation. Prior economic models demonstrated that the risk to *marginal* customers (the edge case) increases when a

vulnerability is announced, even though overall risk to *average* customers decreases (Choi and Fershtman 2005).

When not legally obliged to reveal an InfoSec vulnerability, an organization may choose not to disclose it. Given a choice, managers who only consider the immediate costs of disclosure might choose not to disclose it (Cavusoglu and Raghunathan 2007). Managers have a responsibility to 'do no harm' by avoiding actions that place customers and partners at risk (De George 2008). A customer or partner who is not aware of an InfoSec vulnerability will not know that a fix needs to be installed, and those who become aware of a vulnerability may lack the influence or power to correct the problem (Culnan and Williams 2009).

KANTIANISM AND UTILITARIANISM

In Kant's Theory of Right Conduct, moral requirements are based on reason; an individual who acts in a way contrary to reason is behaving immorally (Kant 1785). Kant's *Categorical Imperative*—the unconditional requirement for autonomous rational beings to respect others' autonomy—dictates that morals are universal; they must be applied uniformly to all rational agents in all situations, regardless of specific features of an individual or of a situation (Kant would not be a fan of contingency theories). Building on the requirements that actions be based on reason and morals universally applied, Kant's Theory of Right Conduct further specifies that an individual must not treat himself or other human beings solely as a means to an end; morality requires us to respect humanity, treating it as an end in itself (Timmons 2012). It is, however, acceptable to use another human as a means to an end, so long as the other party gives informed consent (not consent based on deception or coercion). The principle of universalizability can be applied to test if an action respects others or treats others as a means to an end.

Table 1 compares Kantianism versus Utilitarianism, drawing on prior work by Timmons (2012).

Table 1 Comparison of Kantianism and Utilitarianism (Timmons, 2012)

Kantianism	Utilitarianism
Kant's Theory of Right Conduct provides guidance for judging whether an action is obligatory, wrong, or optional (Timmons 2012): An action A in circumstance C is *obligatory* if and only if (and because) failing to perform A in C would (from among the alternative actions open to one in C) fail to respect humanity to a greater degree than would any alternative action. An action A in C is *wrong* if and only if (and because) performing A would fail to respect someone's humanity to a greater degree than would any other alternative action open to one in C. An action A in C is *optional* if and only if (and because) either (i) performing A would not fail to respect someone's humanity to a greater degree than would any other alternative action open to the agent in C, or (ii) neither performing A nor failing to perform A in C would involve failing to respect humanity.	Mill's classical view of Utilitarianism provides guidance based on the expected utility of a particular action, as described by Timmons (2012): An action A is obligatory if and only if (and because) A would produce a higher level of utility than would any other alternative action that the agent could perform instead. An action A is wrong if and only if (and because) A would produce less utility than would some other alternative action that the agent could perform instead.

Utilitarianism is based on the idea that the consequences of an act determine if it was right or wrong. Utilitarianism is generally implemented either by evaluating particular acts (*act* utilitarianism) or analyzing codes of conduct (*rule* utilitarianism). Utilitarianism determines the deontic status of an action according to the *utility* or total net intrinsic value of its consequences (Mill 1861). To evaluate an action and determine the best course of action (priorities) one compares the net value of expected outcomes versus expected outcomes from alternative actions; the right action is that which yields the highest overall value (or lowest overall negative outcome) to individuals. Although Utilitarianism has been criticized as a promoting a philosophy

of "the ends justifies the means" (Mingers and Walsham 2010), it continues to exert wide influence. For example, utilitarianism underlies the Association for Computing Machinery (ACM) code of ethics (Walsham 1996), ethical analyses in medicine (Baker and McCullough 2007; Haynes 2002) and law (Posner 1979). Classical Utilitarianism is less sensitive to fundamental rights and justice, which are central to Kant's theories. By starting our analysis through a Kantian lens, we avoid dilemmas in which the greatest good would result from behavior that might otherwise be unethical.

VULNERABILITY DISCLOSURE: ANALYSIS THROUGH TWO LENSES

Here, we first answer RQ1a and RQ2a from a Kantian perspective. Then, in order to establish rules of conduct for the timing of vendors' vulnerability disclosures, we answer RQ1b and RQ2b from the perspective of Utilitarianism. Each moral theory relies on different assumptions, as described above. A two-part ethical analysis that starts with Kant avoids a situation in which we would guide vendors to take actions which might yield greater good (optimal ends) yet entail reprehensible actions (unethical means).

Kantian Analysis of Vulnerability Disclosure

In order to consider *if* a vendor or third party should publically disclose a vulnerability (RQ1a and RQ2a), we evaluate vulnerability disclosure from the Kantian perspective. If a hardware or software producer knows that an IT product contains a specific vulnerability and does not disclose this to customers and business partners, the producer is purposely withholding vital information that customers and partners need to make rational decisions about the product, as well as to make decisions for protecting various information resources, human resources, and other resources. Thus, the act of withholding this information disrespects customers' and

partners' autonomy; they have been denied information needed to make rational decisions. Vendors disclose information about vulnerabilities in their products so that customers and business partners can remediate or mitigate the risks associated with a malicious agent exploiting them. Open and transparent information about IT products respects users' autonomy and capacity for informed consent (Spinello 2010).

If a third party discovers the vulnerability, moral guidance is also universally applicable (per Kant); the same logic that applies to a vendor applies to a third party. If a vendor has a moral obligation to inform a customer or partner about InfoSec vulnerabilities in IT products and services (RQ1a), then a third party has the same universally applied obligation (RQ2a).

Utilitarian Analysis of Vulnerability Disclosure Timing

In order to consider *when* an InfoSec vulnerability should be disclosed, we turn to Utilitarianism. The goal of this second stage of evaluation is to identify timing choices that minimize the aggregate risk to customers and partners. Figure 1 is a graphical model that represents risk associated with a specific vulnerability over time. The risk associated with an unremediated (or unmitigated) vulnerability is represented as ***r***. Once customers and partners know about a vulnerability, they can address it. Some customers rely on prepaid automated updates that immediately fix software related to specific vulnerabilities. Others will not immediately fix their software (mitigation will occur at some variable rate). Also, there is residual risk if a vulnerability cannot be completely mitigated. Therefore, mitigated risk decreases toward a minimum value at a rate of adoption. Our model labels this risk ***r**** and it is represented by the Mitigated Risk line. Before an InfoSec vulnerability is publicly disclosed, a vendor and its customers and partners face the risk that a malicious agent will independently discover it. Prior

research demonstrated this scenario, based on the density and cumulative number of vulnerabilities in a software system and the rate of discovery (Alhazmi and Malaiya 2005; Anderson 2002; Musa and Okumoto 1984; Rescorla 2005). We model *discovery risk* ***d(t)*** as a linear function, indicating that this risk increases every day that third parties (whether malicious agents or legitimate security researchers) continue to search for it. This is represented in the model by the Actual Risk line.

Utilitarianism is concerned with the overall net value of an action; therefore, we depict aggregate risk across a population of customers. In Figure 1, we graphically show that if a vulnerability is known to a vendor but not known publicly, the vendor should wait to disclose it until the point in time when mitigated risk is equal to the likelihood that the vulnerability will be independently discovered. We label this point **A** on the model. At this point the risk **r*** equals ***d(t)*** and the risk decreases as the vulnerability is mitigated through customers' and partners' remediation efforts. However, when a vulnerability is known to the vendor but *not* disclosed to customers and partners (at point B), the net risk for customers is higher than it would have been if the vendor disclosed earlier. If the vulnerability is never disclosed and is not remediated, the risk level remains at ***r*** which represents the probability of an attacker exploiting the vulnerability.

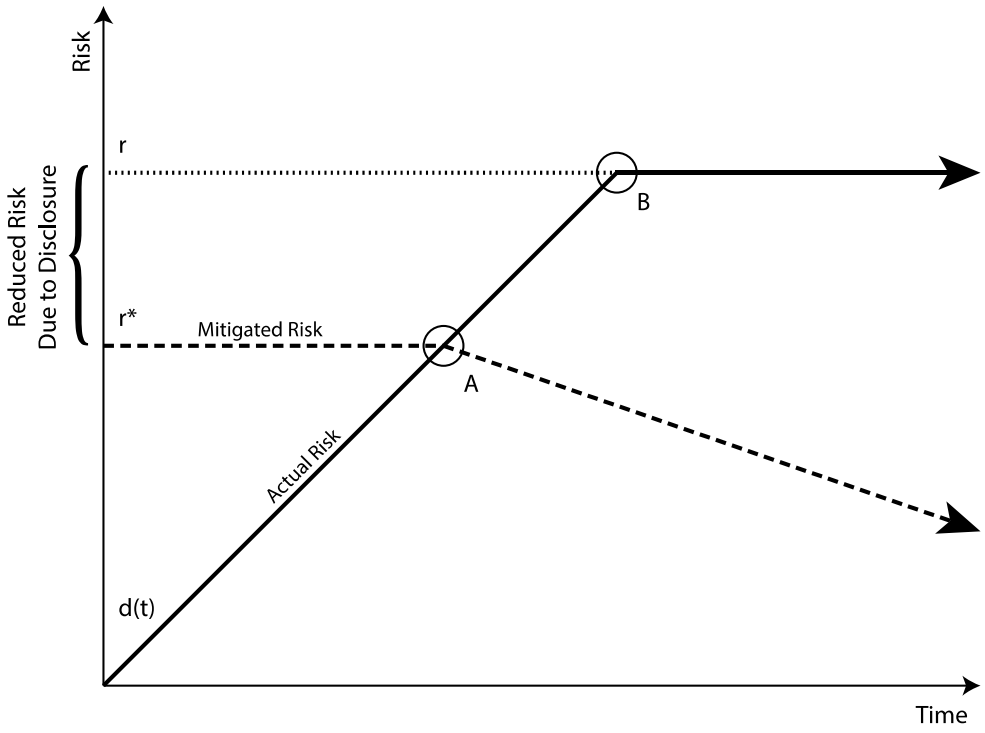

Figure 1: Aggregate Risk of Vulnerability Disclosure Timelines

In Figure 1, the difference between ***r*** and ***r**** represents the reduction of risk due to disclosure. This risk may be immediately reduced through mechanisms such as automatic updates. Risk can be further reduced as customers and partners continue to learn about the issue and take care of it (such as by upgrading their software to a version where this vulnerability has already been fixed, or investing in contingency plans for dealing with the consequences if an unfixed vulnerability is exploited). Four different areas of Figure 2 (below) represent varied risk levels. The unshaded upper left quadrant represents unrealized risk. The blue upper-right quadrant represents risk due to non-optimal or late disclosure (vendor releases a fix after a malicious agent discovers it).

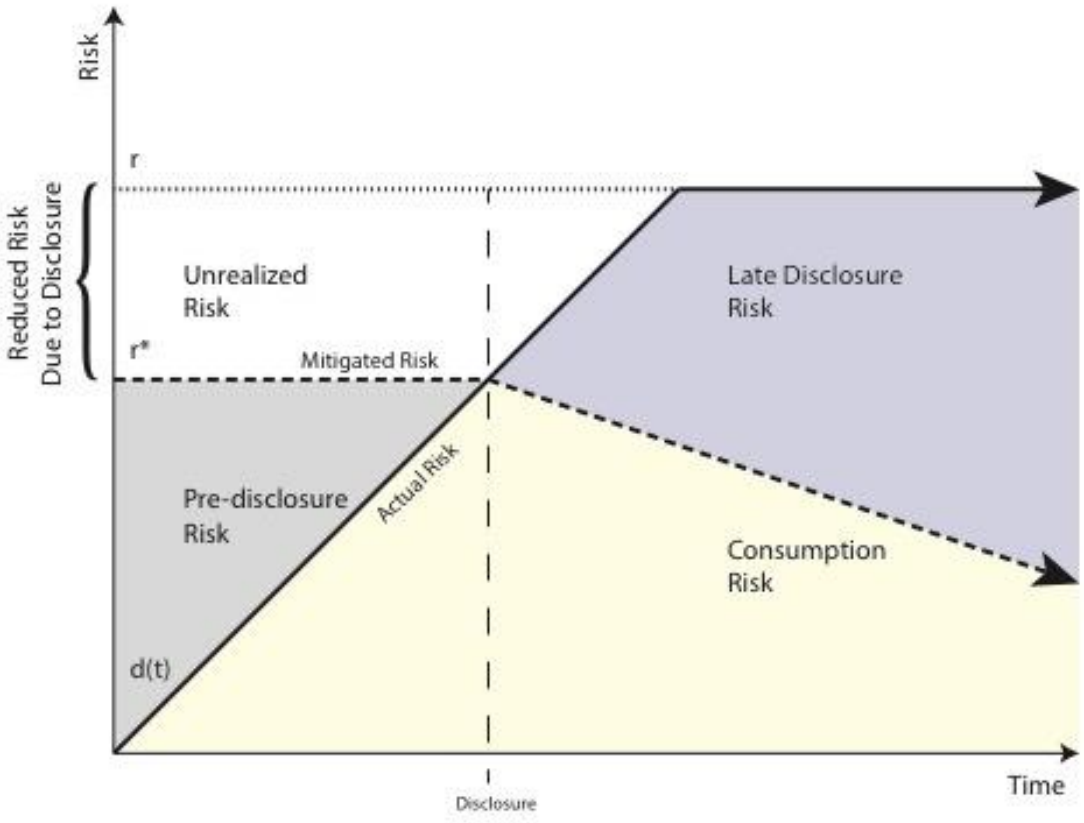

Figure 2: Risk Quadrants of Modeled Risk Disclosure

The gray, bottom-left quadrant of Figure 2 depicts the case in which a vendor discloses the vulnerability before its likely independent discovery by a malicious agent. Disclosure is morally wrong in the gray and blue areas, since it would place the user population at higher risk (lower utility) than the alternative act of non-disclosure. The yellow area represents the mitigated risk that customers face due to their ongoing consumption of the product. Here, is where vendors *ought* to disclose IT vulnerabilities.

DISCUSSION

Managers aim to make decisions that provide benefits to various stakeholders while remaining ethical. Application of Kant's Theory of Right Conduct reveals that IT product vendors must

disclose information about known InfoSec vulnerabilities in their products and services, but it does not readily address how quickly a vendor should disclose and remediate a vulnerability. More empirical research and simulations are needed to quantify risks of undisclosed vulnerabilities under different discovery models. Our model assumes managers and third parties will immediately know when one or more malicious agents discover a particular vulnerability (point A on Figures 1 and 2). Since information about malicious agents' knowledge is not always known, it follows that vendors should make every effort to fix and disclose vulnerabilities in a timely fashion, and vendors should also take steps that aim to motivate customers to install each fix. Our model also demonstrates that in order to minimize risk to a population of customers and business partners, a third party should only be a first discloser if they can provide a complete fix for the vulnerability. Previous studies reported that external pressure (in the form of third party disclosures) may motivate organizations to provide timely fixes (Arora et al. 2010). If everyone respects humanity as Kant proposed and everyone attempts to minimize the potential for negative outcomes (per Utilitarianism), customers and partners would be better off. However, the moral compass of managers and external parties doesn't always point to true north. Therefore, third parties who attempt to take the moral high ground regarding vulnerability disclosure must work in good faith with one another to produce fixes, make them quickly available to customers and business partners, communicate the necessary information to motivate customers to adopt the fixes, and refrain from imposing authoritarian timelines. In essence, non-malicious third parties and vendors should work together and adopt a policy of coordinated disclosure.

REFERENCES

Alhazmi, O. H., and Malaiya, Y. K. 2005. "Quantitative vulnerability assessment of systems software," in *Proc. annual reliability and maintainability symposium*, pp. 615–620.

Anderson, R. 2002. "Security in open versus closed systems—the dance of Boltzmann, Coase and Moore," *Open Source Software Economics*.

Arora, A., Krishnan, R., Telang, R., and Yang, Y. B. 2010. "An Empirical Analysis of Software Vendors' Patch Release Behavior: Impact of Vulnerability Disclosure," *Information Systems Research* (21:1), pp. 115–132.

Arora, A., Telang, R., and Xu, H. 2008. "Optimal policy for software vulnerability disclosure," *Management Science* (54:4), pp. 642–656.

Baker, R., and McCullough, L. B. 2007. "Medical ethics' appropriation of moral philosophy: The case of the sympathetic and the unsympathetic physician," *Kennedy Institute of Ethics Journal* (17:1), pp. 3–22.

Cavusoglu, H., Cavusoglu, H., and Raghunathan, S. 2005. "Emerging Issues in Responsible Vulnerability Disclosure," Presented at the Workshop on the Economics of Information Security, Boston, MA.

Cavusoglu, H., and Raghunathan, S. 2007. "Efficiency of vulnerability disclosure mechanisms to disseminate vulnerability knowledge," *Software Engineering, IEEE Transactions on* (33:3), pp. 171–185.

Choi, J. P., and Fershtman, C. 2005. "Internet security, vulnerability disclosure and software provision," Presented at the Workshop on the Economics of Information Security, Boston, MA.

Culnan, M. J., and Williams, C. C. 2009. "How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches," *MIS Quarterly* (33:4), pp. 673–687.

De George, R. T. 2008. *The ethics of information technology and business*, John Wiley & Sons.

Dhillon, G., and Backhouse, J. 2000. "Information system security management in the new millennium," *Commun. ACM* (43:7), pp. 125–128.

Grossman, S. J. 1981. "The informational role of warranties and private disclosure about product quality," *Journal of Law and Economics*, pp. 461–483.

Haynes, R. B. 2002. "What kind of evidence is it that Evidence-Based Medicine advocates want health care providers and consumers to pay attention to?," *BMC Health Services Research* (2:1), p. 3.

Kant, I. 1785. *The moral law: Groundwork of the metaphysic of morals*, Psychology Press.

Leiwo, J., and Heikkuri, S. 1998. "An analysis of ethics as foundation of information security in distributed systems," (Vol. 6), Presented at the System Sciences, 1998., Proceedings of the Thirty-First Hawaii International Conference on, IEEE, pp. 213–222.

Mill, J. S. 1861. *Utilitarianism*, Broadview Press.

Mingers, J., and Walsham, G. 2010. "Toward ethical information systems: the contribution of discourse ethics," *MIS Quarterly* (34:4), pp. 833–854.

Musa, J. D., and Okumoto, K. 1984. "A logarithmic Poisson execution time model for software reliability measurement," in *Proceedings of the 7th international conference on Software engineering*, IEEE Press, pp. 230–238.

Posner, R. A. 1979. "Utilitarianism, economics, and legal theory," *The Journal of Legal Studies*, pp. 103–140.

Rescorla, E. 2005. "Is finding security holes a good idea?," *Security & Privacy, IEEE* (3:1), pp. 14–19.

Spinello, R. 2010. *Cyberethics: Morality and law in cyberspace*, Jones & Bartlett Learning.

Timmons, M. 2012. *Moral theory: an introduction*, Rowman & Littlefield Publishers.

Walsham, G. 1996. "Ethical theory, codes of ethics and IS practice," *Information Systems Journal* (6:1), pp. 69–81.