



On risk: perception and direction

Andrew Stewart

Received 28 April 2004; revised 4 May 2004; accepted 4 May 2004

KEYWORDS

Information security;
Risk;
Metrics;
Risk assessment;
Security assessment;
Vulnerability
assessment;
Risk compensation;
Risk homeostasis;
Precautionary
principle

Abstract The idea of risk permeates the information security field. We use terms like “risk management”, “risk assessment”, “risk model” and “risk analysis” every day, and those topics are themselves the subject of countless papers and articles in security journals and magazines.

But has the concept of risk become so ingrained within our profession that we have become over confident about how much we really understand it? In this paper I discuss how difficult it is to truly understand risk. I describe why we need to fundamentally reassess many of our current activities that involve trying to calculate and manipulate risk. I also make several proposals for how we can collectively treat risk in a more pragmatic and realistic way.

© 2004 Published by Elsevier Ltd.

“To defend against the worst case will quickly bankrupt any imaginative government”—William Nordhaus

“If a guy tells me the probability of failure is 1 in 10^5 , I know he’s full of crap”—Richard Feynman

Introduction

The goal of this paper is to highlight the complexities in a particular area of study within the information security field, namely risk assessment. The purpose is to attempt to mitigate the negative effects on the field that a complacent attitude to this subject creates.

The section “Calculating risk (or trying to)” describes the fundamental difficulties involved

when attempting to calculate the risk associated with security vulnerabilities. The section “[Risk metrics for the real world](#)” explains the benefits of using *comparative analysis* to provide a pragmatic alternative to existing approaches that attempt to quantify risk.

The section “[Risk compensation theory](#)” describes the theory of *risk compensation* using several real-world examples. The applicability of risk compensation theory to the task of delivering effective information security within an organization is discussed. The *precautionary principle* and the sociological aspects of risk compensation theory are described in the section “[Sociological aspects of risk compensation theory](#)”. The section “[The commercialization of risk assessment](#)” explains why the commercialized view of risk assessment often neglects important factors.

In the section “[Risk mindsets and language](#)” some common views of risk are analyzed, together with the use of language related to risks. The

E-mail address: andrew_j_stewart@mac.com.

section “[New directions](#)” makes recommendations for how companies, security professionals, and the security industry can adopt a more realistic and ultimately more beneficial view of risk.

Calculating risk (or trying to)

A “risk assessment” is a very common information security activity. The commonly understood information security lifecycle incorporates risk identification as a key component. Much of the commercial information security industry is concerned with the identification of risks, specifically those created by software vulnerabilities.

The goal of a risk assessment is usually to find vulnerabilities so that they can be patched; a methodology sometimes referred to as “penetrate and patch”. Whether the subject of a risk assessment is an entire business or a single piece of software, the end result is inevitably that a number of security vulnerabilities are found.

Given that vulnerabilities exist, it is logical to ask: what is the *risk* associated with those vulnerabilities? It seems to make sense that if we know the level of risk that exists then we can make recommendations for how to work to appropriately mitigate that risk.

To calculate the level of risk, we need to know how likely it is that the perilous event associated with that risk will occur; i.e. how likely it is that a particular vulnerability will be exploited. If I want to insure my house I can contact an insurance company and they will give me a quote based on a calculation of the probability that my house will burn down, be destroyed by a tornado or suffer some other disaster. The insurance company can make that risk calculation because they have a vast amount of actuarial data concerning the probability of those events occurring based on what they have observed and recorded in the past. Their false-positive rate (fraudulent house insurance claims) and false-negative rate (instances where someone’s house burns down but they do not make a claim) are low enough not to affect the veracity of their model.

But in the case of trying to determine the probability of an attack against a computer system, we have no reliable historical data with which to make a similar calculation. The FBI and other organizations make yearly surveys of computer crime ([Computer Security Institute, 2003](#)), but the data from those reports is based on crimes that have been *voluntarily* reported. It is not unreasonable to presume that a large amount of computer crime

goes unreported because of worries about liability or possible damage to reputation. The FBI surveys are also high level to the extent that they are not specific to individual security vulnerabilities.

There is no mechanism that mandates the wide-scale reporting of security activity such as security incidents and break-ins, and it is therefore impossible to calculate the possibility of a future attack on the basis of past activity.

Consider also that the process of attacking and defending computer systems is infinitely reflexive. We modify our defenses in response to attackers who modify their attack in response to our defenses, and so on ad infinitum. This shifting landscape makes any risk calculation extremely difficult because the parameters of the equation are altering rapidly over time. Attempts to model attacker’s actions in an abstract, mathematical way and then to attempt to predict the future actions of attackers based on those models is a problem that is non-trivial and is currently unsolved.

There is no reliable past data from which to make predictions. It is extremely difficult to create a mathematical model that would predict attacker’s actions. It is therefore a fallacy to say that we can calculate the risk of a given vulnerability being exploited. If you know the probability that a perilous future event will occur, that is a measurable risk. If you do not know the probability, that is not a risk, that is *uncertainty*. When facts fall short of certainty we make assumptions, we infer, and we fall back on our beliefs, but supposition cannot take the place of facts. Intuitively we would seek to improve the quantity and quality of information that is available to us so that we can make better decisions about risks, but the software defects that give rise to security vulnerabilities are both omnipresent (they are in every piece of software) and nascent (they lie dormant for years).

Risk metrics for the real world

As a field, our assumption always seems to be that the current level of risk is too great. But overestimations of risk can lead organizations to waste huge amounts of money trying to secure systems that are unlikely to ever be attacked. Excessive and burdensome security measures introduced because of inflated perceptions of risk can stifle productivity. Overestimates of risk can also wrongly encourage companies to focus on more non-electronic ways of doing business. As security professionals it is our responsibility to provide

a balanced perspective, and yet the current culture of our field points us in one direction only: more security.

Consider a company that has just completed a vulnerability assessment and has discovered the existence of 210 vulnerabilities within its environment. Over two hundred vulnerabilities certainly *sounds* bad, but is the situation really as gloomy as it appears? Patching vulnerabilities and putting security measures in place inevitably involves cost. All security measures have an associated cost, and so if a particular company has 210 vulnerabilities and that company's competitors share an average of say, 630 vulnerabilities, then perhaps the company is already spending *too much* on security; money that could have been spent making the company more competitive. That thinking may seem heretical to those in the security field, but companies think and operate in exactly those terms.

If our goal is to recommend security measures that are pragmatic, and we acknowledge that we cannot accurately calculate the risk that a given vulnerability will be exploited, what alternative approaches can we employ? One approach is to employ *comparative analysis*.

Comparative analysis is the ability of an organization to compare a measure of its security to its peers. This capability is already offered by some collaborative organizations as a service. The [Information Security Forum](#) is a non-profit association that allows companies to partake in a comparative security ranking, based on a series of questionnaires which the participants complete using the honor system. (The resulting rankings are blind between companies for confidentiality.) This service allows a company to discover if they rank, say, seventh out of their 50 peers, or forty-seventh. In my experience, this ranking is perceived by companies to provide far more value than simply being told that they have *X* number of security vulnerabilities, because "*X* vulnerabilities" provide no context from which to infer a reasonable course of action.

This idea of comparative analysis could be applied to a multitude of existing security services and products with relatively little effort. Companies that perform managed security monitoring and vendors of patch management software are two examples where a by-sector trend analysis of data would provide great value to the participants (customers).

The philosophical question of "How much security is enough?" is often bandied about in the security field because in a theoretical sense it is a very difficult question to answer. From a business

perspective however, the answer could well be: *At least as much as your average competitor.*

Risk compensation theory

Most security programs within companies have the high level goals of "protecting against risk", "managing risk", "driving down the level of risk" and other variations thereof. But many people working in the information security field have had experiences within companies that have been very frustrating because it seems that as soon as security measures are implemented, the company does something to invalidate them or it makes a mistake somewhere where the security measures do not extend. Is there a theory that can explain this phenomenon? It turns out that there is; it is the theory of risk compensation.

Risk compensation theory is sometimes referred to as risk homeostasis or behavioral adaptation. It is the idea that after safety measures have been introduced, the level of risk is re-asserted at the level with which the subject was originally content. This means that after you introduce a security measure to a system where the current level of security is perceived to already be acceptable, the level of security does not go up, it actually stays the same. The risk does not go away; it gets redistributed around the totality of the system.

This is a somewhat counter-intuitive idea, and so I will describe several real-world examples.

An example of risk compensation theory in action in the physical world is with seatbelt legislation. No one can deny that if you are in a car crash you are more likely to survive if you are wearing a seatbelt, but risk compensation theory suggests that because people are required by law to wear seatbelts they compensate subconsciously by driving more recklessly. Field data support this hypothesis. The number of automobile-related deaths in the United Kingdom actually went *up* after seatbelt legislation was introduced, and there was also an increase in the deaths of pedestrians ([Adams, 1999](#)). Arguably, the effect of introducing the safety measure transferred the risk to a more vulnerable subset of society.

Another example of risk compensation can be found in the sport of skydiving. Several years ago a European company created a device which will automatically deploy a skydiver's parachute if for some reason the skydiver does not. For example, if the skydiver is knocked unconscious when exiting the plane, the device will deploy the reserve parachute at a certain altitude. This device has saved

many skydivers' lives by greatly reducing the number of deaths caused by no parachute being deployed. However, if you plot the reduction in those types of death year-on-year together with deaths in the sport caused by other reasons, it can be seen that there is an almost exact inverse relationship. The number of deaths in skydiving has remained broadly equivalent each year (taking into account the increasing number of participants in the sport), but the nature of the deaths has shifted (Napier, 2000). This finding is in alignment with risk compensation theory because it predicts that, essentially, skydivers will compensate for any new safety mechanism and consequently perform more dangerous types of jumping.

In Oslo, a study of the driving behavior of taxicab drivers found that drivers who drove cars equipped with ABS (anti-lock brakes) drove significantly closer to the car in front, compared to cars which were not equipped with ABS, thereby nullifying the safety benefit of the technology (Fosser et al., 1997). Another study on the effects of ABS in Munich tracked two equal sized sets of cars. The cars in each set were of the same make and were identical in all respects other than the presence or absence of ABS. Taxicab drivers were randomly assigned a car that had ABS or did not. Over the three year period of the study, 747 car accidents were recorded, and there were more accidents that involved cars *with* ABS than cars without (Aschenbrenner and Biehl, 1994).

In the field of insurance the idea of risk compensation is known as "moral hazard". When someone is insured they often compensate by taking greater risks than they would ordinarily do, because they know that their insurance protects them financially. The insurance company may therefore receive more claims than their models predict. From a clinical perspective, fire insurance actually provides an incentive to commit arson if the payoff is greater than the value of the property. Most police investigations into arson are the result of leads from suspicious insurance adjusters.

The final example I will present is a 10 year long study that was performed on the subject of cigarette smoking. People in the study who stopped smoking suffered less instances of lung disease, but the overall life span of that group was actually shorter than the smokers who continued to smoke (Rose, 1982). Similarly, smokers who were given low-nicotine cigarettes maintained their nicotine level by inhaling more frequently and more deeply (Warner and Slade, 1992).

These scientific studies show that attempts to reduce risk are continually frustrated where the subject's target level of risk is already deemed

satisfactory by the subject. Of course, correlation does not prove causation. Just because two trends occur simultaneously does not mean that one is causing the other. On the other hand, data from the studies referenced above seem to align with the frustration that many security practitioners have felt when trying to improve security within different organizations. The feeling that companies are "stubborn" regarding impending or existing security measures seems to be common among security practitioners.

There are many documented examples where the security of a system failed because the security measures that were in place were relied on too heavily, gave too much of a false sense of security or were used as an excuse to not employ security in other areas. The Davy Lamp, a miner's safety lamp, is usually described as having saved thousands of miner's lives because it operated at a temperature below the ignition point of methane. But the lamp enabled the extension of mining into previously unreachable methane-rich atmospheres and so the introduction of this "safety" device was followed by an increase in the number of gas explosions and deaths (Glassner, 1999). Compare that scenario to the classic example of reliance on a firewall and perimeter security to justify not hardening the security of internal systems on a network. Firewalls, encryption, intrusion detection systems and many of the other tools and techniques within the security profession have all suffered this same fate of over-reliance.

What then, can risk compensation theory teach us about how to approach the task of delivering effective information security within an organization? If we look at the way that companies view information security we can see that risk compensation theory predicts many of their actions. A security incident tends to spur an organization to attempt to increase security, but then the enthusiasm for security within the organization tends to wane over time as the incident recedes in the organization's collective memory and the acceptable level of risk is reset at the original value. Because security professionals live and breathe security, their goal for the level of acceptable risk within a company usually does not match the company's perception of the acceptable level of risk. In its worst stages, this affliction can result in a state of deadlock between the internal security group and the business.

If risk compensation predicts that the cycle of boom and bust is inevitable with regards to the perception of risk, then the only way to make a security program effective—to not let it be led by the emotion of reacting to whatever is perceived

to be the latest and greatest risk—is to *institutionalize* security. By institutionalize, I mean integrate security within the core of the business such that security becomes an element within the strategic decision making process. I am not suggesting that information security needs to become a core competency for every company, but it needs to be an element that is considered just as financial regulatory compliance and public relations are always considered when making key business decisions.

An example of the necessity of this approach is with safety legislation related to cycling helmets. In 1992 a law was passed in Western Australia that made the wearing of a helmet compulsory when riding a bicycle. Predictably, this law did not have the intended effect of reducing deaths, since the number of fatalities remained at the same level, post legislation (Hillman, 1993; <http://www.cyclehelmets.com>). In the Netherlands there are a greater number of cyclists than in Australia. Relatively few of them wear helmets, and yet their fatality and injury rates are very low in comparison. The crucial difference is that in the Netherlands they have sought to create an environment in which accidents are less likely to occur by employing strategies such as creating dedicated cycle-lanes.

The approach taken by the Western Australian government to attempt to increase the safety of cyclists parallels the attempts of many security teams to improve security within their companies. But as the examples above have shown, the path to effective information security cannot be found through trying to enforce policies that attempt to mandate behavior. The subject will merely adjust. Effective information security can only be accomplished through creating an environment in which the participants *transparently* participate in the security process in a way that allows them to retain the notion that they are operating at their own internal level of acceptable risk.

Sociological aspects of risk compensation theory

Risk compensation theory can be seen to be at odds with the precautionary principle that exists at the heart of current thinking within the information security field. Adherents to the precautionary principle press for action as a matter of urgency and in the case of information security the latest “threat” or “risk” is usually bandied about as justification. To a certain extent the popularity of this thinking is understandable because our approach to matters is influenced by the company we keep.

Within the security field the more populist journals and magazines tend to have an obsession with describing the latest “threats” and “risks”. Ideas that are convenient to express often gather momentum and become populist.

The precautionary principle is in direct opposition to the social vocabulary of risk that exists in the world at large. That vocabulary includes such slogans as “no risk, no reward”, “just do it”, “no guts, no glory”, “no fear”, and “no pain, no gain”. Individuals who take risks such as sportspeople and entrepreneurs are glorified and practically worshiped within society and so advocates of the precautionary principle have to constantly fight an uphill battle against that weight of influence.

Participants in any collaborative activity become part of a social group, and every social group creates its own set of concepts, practices and vocabulary that define the group’s collective approach to the activity. As a field, we view risk almost as a commodity that can be seen, measured, apportioned and manipulated at will. But even the relatively short analysis within this paper suggests that risk is a more subtle concept than perhaps the center of the field considers it to be. Breaking this group-think will be difficult because the commercial security industry relies to a large extent on a simplistic view of risk that can be easily commoditized and sold.

The commercialization of risk assessment

There are many security companies that offer “free” security assessments precisely for the reason that the odds are in their favor that they will find at least some security vulnerabilities. They can then leverage the existence of those vulnerabilities to convince the customer that they have to invest in additional security measures. This is an aspect of the commercial information security industry that we should acknowledge and address, because the practice can be predatory and not beneficial to companies.

Dependency is a crucial dimension of risk that is often not considered as part of risk assessments or is ignored for political reasons. Every company has dependencies on multiple third parties such as their upstream ISP, Telco provider, contractors, outsourcing organizations, and so on. Dependencies are risks because, by definition, if you depend on someone then they could act in a way that negatively impacts you. We can consider risks that arise out of dependency to be “indirect” risks rather than “direct” risks. Direct risks tend to

have an “in your face” nature, such as with well-publicized security vulnerabilities in operating systems or popular applications. Indirect risks tend to be more subtle and only emerge when you analyze business processes and not just the technology components of an infrastructure.

Many security assessments only consider direct risks and not indirect risks. There are two reasons for this, both of which have their roots in the way that security is both marketed and perceived. Firstly, indirect risks are not as easy to leverage as direct risks for pursuing the goal of securing future security work off the back of a security assessment. It is much easier for a security consulting firm or a security product vendor to say: “These are your vulnerabilities, now pay us to help you fix them”, than it is to paint the bigger, contextual picture in which it is the nature of an organization’s environment and its day-to-day operations that creates the greatest potential for loss. Secondly, organizations are not savvy enough to request that security assessments include a consideration of indirect as well as direct risks. “Management by magazine article” is a very common occurrence when it comes to provisioning security services and technologies, and the verbiage that the commercial security industry puts out generally does not dwell on areas that are not perceived to be translatable into immediate commercial gain.

It is true that in many companies the internal security organization has no visibility into the business processes that create indirect risks. This will most likely change in the future through an increasing reliance on the contractual definition of accountability for security, i.e. by necessitating security criteria within service level agreements.

The risks to information cannot usually be seen in the same way as risks to our physical bodies (such as an oncoming truck). The fact that information risks are often unclear and unquantifiable allows them to be manipulated to advance an agenda. Fear is a great motivating factor. If you want to motivate a person or a company, one way to do it is to make them afraid by highlighting risks and then present yourself as the solution. The emotional connotation of the word “risk” carries a lot of weight in decision making. As a field, we have used “risks” to collectively advance our agenda, but in doing so we have built a sizable part of our profession on uncertain ground.

Risk mindsets and language

Some parts of the security community portray security as an “all or nothing” affair. Certain operating systems or applications are deemed

“secure” whereas others are not.¹ This absolutist approach is the logical extreme of the precautionary principle. It is akin to a professional body-builder being unable to comprehend how someone could possibly bring themselves to eat a donut. The reality is that that kind of thinking will always be viewed as radical by the world at large—i.e. by the companies within which we are trying to create change. We need to approach people on their own terms and in a way that does not create the impression that complex topics such as security and risk are binary issues.

Even though most security professionals understand that it is impossible to reduce the level of risk to zero, the commercial security industry often holds up the goal of zero risk as an ideal. This is most prominent in print advertising for security products. When companies promote “total security protection” or claim to be able to provide “security’s silver bullet”, they do the security field a disservice because by making those claims they promulgate the idea that a panacea exists; that there is a nirvana state of security that can be reached by installing a particular product or by using a specific service.

The media also plays a significant role in shaping the perception of risk. Wireless networking has received very bad press related to the security vulnerabilities within the de facto wireless technical standards such as WEP. The archetypal risk to wireless networking is “war driving” in which an attacker accesses a company network from outside the physical perimeter of the company facility. Many companies are so concerned with this risk that they have banned all wireless networking from their entire organization.

Studies have shown however, that when presented with several descriptions of the dangers inherent in a given situation, people tend to move toward the most alarming account (Kip Viscusi, 1997; Slovic et al., 2000). In other words, reaction to risk is most influenced by the severity of the possible outcome.

Can every company expect to be exposed to the same levels of risk associated with certain technologies or activities? Do we expect that the risk of a security compromise via a wireless network is the same for a manufacturing company in a semi-rural location as it is for a telecommunications company in a metropolitan location? A pragmatic analysis of that situation would likely be that the relative level of risk is not similar, and yet such

¹ A significant contributing factor to such a mindset is elitism related to operating system preference.

factors are often eclipsed in the risk analysis process by the mere possibility of the “worst case scenario”. We should seek to communicate risks in a way that accounts for both the technical aspects of the issue and the participant’s likely subjective impression of the potential impact (French et al., 2003).

To be fair, as individuals we sometimes also make similar misjudgments about risk. Consider the fear that many people feel when flying in a commercial airline, yet compare that level of anxiety with the nonchalance we feel when traveling in a car. Fewer than 13,000 people have been killed in the entire history of aviation accidents dating back to 1914. The amount of people killed in car accidents in the US is three times that number every single year (Glassner, 1999). Our belief in how much risk exists in any given situation is clearly influenced by emotional factors that affect our *perception* of the level of risk. You can tell someone who is afraid to fly that the chances of being killed in a plane crash is roughly 1 in 4,000,000, but being presented with that statistical reality probably will not make that person feel any better about flying. What we *feel* often wins out over any objective analysis that we are presented with.

The benefit or cost created by the role that the media plays in popularizing certain risks, and the extent to which the commercial information security industry contributes to that process, is currently unclear. There may be more cost than benefit.

New directions

Given the issues that this paper has discussed, how should we, as professionals and as a profession, treat risk?

For security professionals

- It is our obligation to admit the reality that it is difficult, perhaps impossible, to calculate the real “risk” of a computer system being attacked. Revealing this fact does not invalidate any other consultative advice that we might give, because noting areas of weakness within an approach is an important part of the scientific method. The true weight of a risk is the combination of multiple factors, many of which are purely subjective. The truth is that we are all guessing. If we knew for certain it would not be risk we were dealing with.

- As security consultants we are often presented with two choices when dealing with our clients: to simplify an issue or to attempt to describe its true complexity. In many situations it is tempting for us to present the answer to a security problem in a way that allows us to subsequently provide the “solution”. The level of security knowledge within most organizations is usually slight, and so we can coast on our greater level of knowledge and usually get our way. Our professional responsibility however, is to describe the complex reality of security problems and not to package them up in ways that lend themselves to fake, silver bullet solutions. As the level of security knowledge goes up (through a process of accumulation if nothing else), organizations will start to be able to see through any such over-simplifications.
- We have no accurate measure of how many security incidents are actually occurring, but whatever the number is, it reflects the propensity of companies to willingly take risks. We cannot ignore the possible rewards that can come from taking a risk. If you have ever driven faster than the speed limit then you have risked receiving a speeding ticket, but you have accepted that risk for the perceived benefit. We will continuously be frustrated if we try to make companies more secure than they want or need to be.
- Risk compensation theory suggests that attempts to increase security, such as by deploying technologies or through attempts to mandate policy, will be continually frustrated where the subject perceives the level of security to already be sufficient. The only way to circumvent that result is to transparently build security into the everyday existence of the subject, and to do so in a way that is not perceived by the subject to create an impediment.

For companies

- Companies should be made aware that vulnerability assessments are often pitched for ulterior motives (usually the hope that vulnerabilities will be found so as to be able to recommend products and services to “mitigate” those vulnerabilities).
- There is more value to a company in determining the extent of indirect risks that arise out of business activities (such as through

connectivity with third-parties) than in focusing on the endless stream of “latest and greatest” vulnerabilities.

- Security incidents tend to manifest as technology problems, but they usually have their roots in people and process deficiencies. A colleague once told me of a company who had an impressive ACL (access control list) on their edge router, but within the configuration of the router the ACL had never been applied to the external interface. Each week the security staff would diligently add entries to the ACL, not realizing the utter pointlessness of their effort until a third-party discovered the oversight. The risks that arise from that example, as in many cases, can only be addressed through effective operational processes that surround the day-to-day activities related to security.

For the security industry

- The commercial information security industry glosses over many of the complexities described in this paper because “calculating” risk and then apportioning corrective measures (i.e. products and services) is currently the most effective sales technique they feel they have. If you, as a company, do not have a problem (i.e. risks that you need to mitigate) then it becomes very hard to sell you a product or service to “solve” that problem. This is not a beneficial strategy for the security field in the long-term because the issues that we should be attempting to address are the deep rooted ones. By its very nature, the “penetrate and patch” paradigm only addresses superficial, usually fleeting problems.
- We need to recognize that placing a lot of emphasis on highlighting the constant stream of new “risks” contributes greatly to the perception that the only way we can justify our existence is by perpetuating FUD (fear, uncertainty, and doubt). Again, this is not a sustainable approach.
- Companies are unlikely to voluntarily release data related to the number of security vulnerabilities within their environment, nor information related to successful security compromises, even though such data would be tremendously valuable when viewed in the round. One approach would be to lobby government to mandate the disclosure of such information, but this tactic would be unadvisable at best. A better approach is to encourage companies to generate and submit

that information voluntarily by creating incentives for them to do so, such as participation in comparative analysis that would provide comparative “rankings” on a by-sector basis, for example. For the information security industry this would shift the burden away from constantly trying to “sell” security as a reaction to the latest security risk and towards an incentivized pull for security from within companies themselves.

- Companies must eventually grow tired of being forced to work within the “penetrate and patch” model. When that turn occurs they will seek to identify and attack the real roots of security problems, either with the help of the security industry or without it.

References

- Adams J. Cars, cholera, and cows: the management of risk and uncertainty. *Policy Anal* March 4, 1999;335.
- Aschenbrenner M, Biehl B. Improved safety through improved technical measures? Empirical studies regarding risk compensation processes in relation to anti-lock braking systems. In: Trimpop RM, Wilde GJS, editors. *Challenges to accident prevention: the issue of risk compensation behavior*. Groningen, the Netherlands: Styx Publications 1994.
- Computer Security Institute. 2003 CSI/FBI computer crime and security survey; 2003. Available from: <http://www.gocsi.com>.
- Fosser S, Saetermo IF, Sagberg F. An investigation of behavioral adaptation to airbags and antilock brakes among taxi drivers. *Accident analysis and prevention*, vol. 29. Available from: <http://www.sciencedirect.com> [Issue 31].
- French S, Maule J, Mythen G. Food risks: integrating effective risk communication into the risk management process (draft); 03/09/2003.
- Glassner B. *The culture of fear; why Americans are afraid of the wrong things*. Basic Books; 1999.
- Hillman M. Cycle helmets: the case for and against. *Policy Studies Institute*; 1993. Available from: <http://www.pcug.org.au/~psvansch/crag/psi.htm>.
- Available from: <http://www.cycle-helmets.com> on 3/25/2004.
- Information Security Forum. Available from: <http://www.securityforum.org>.
- Kip Viscusi W. Alarmist decisions with divergent risk information. *Econ J* Nov., 1997;107(445):1657–70.
- Napier V. Open canopy fatalities and risk homeostasis: a correlation study. Western Oregon University; March 5, 2000. Available from: <http://www.noexcusesrigging.com/EssaysArticles.htm>.
- Rose G, Hamilton PJS, Colwell L, Shipley MJ. A randomised control trial of anti-smoking advice; 10-year results. *J Epidemiol Commun Health* 1982.
- Slovic P, Monahan J, MacGregor DG. Violence risk assessment and risk communication: the effects of using actual cases, providing instruction, and employing probability versus frequency formats. *Law Hum Behav* June 2000;24(3).
- Warner KE, Slade J. Low tar, high toll. *Am J Public Health* 1992.

Andrew Stewart has worked in the information security field for over 10 years. He has held information security positions at Deutsche Bank, Internet Security Systems, Barclays Capital, and Reuters. As a consultant he has acted as a trusted security advisor for companies in numerous vertical markets including finance, healthcare, law, construction, government, non-profit, manufacturing, consulting, and telecommunications.

He has lectured to government, corporate, financial and special interest audiences on both the technical and managerial aspects of the information security discipline.

Andrew holds the CISSP (Certified Information Systems Security Professional) certification, and is a member of the ACM, IEEE, ISSA, and USENIX. Andrew received his Bachelor of Science degree in Computer Science from Oxford Brookes University in Oxford, England.

Available online at www.sciencedirect.com

