



MAKING THE CASE FOR REPLACING RISK- BASED SECURITY

By **Donn B. Parker, CISSP**
donnlorna@aol.com

Note: This article contains the opinions of the author, which are not necessarily the opinions of the ISSA or The ISSA Journal.

IT trade publications are increasingly reporting the failings of risk management and risk assessments. According to some IT trade journals, information security is under-funded and under-staffed. Legislators are now imposing security bylaws and regulations just as they did with seat belts long ago. These legislative actions also seem to be a reaction to possible failure of the information security practice. What are we doing wrong? Is the lack of support for adequate security linked to our risk-based approach to security? Why can't we make a successful case to management to increase the support for information security to meet the needs? Part of the answer is that management deals with risk every day, and it is too easy for them to accept security risk rather than reducing it by increasing security that is inconvenient and interferes with business. We need to make it imperative and unavoidable that they support reasonable levels of security by emphasizing due diligence to avoid negligence, compliance

with law to avoid penalties, and enablement to be competitive. Reduction of security risk then becomes serendipitous.

It is relatively easy to justify increased security to stop ongoing loss, incidents and attacks from computer viruses, worms, and identity theft because the losses are significant, visible, happening now, and the benefits of security are obvious when the incidents stop or are controlled. The problem is making a successful case for adequate security to protect from rare incidents such as enemies engaged in fraud, embezzlement, espionage, theft of trade secrets, violation of privacy, denial of service, extortion, and other attacks that may not happen often but tend to result in relatively significant losses. There seems to be no urgency until a loss occurs, and then it is too late, written off, and soon forgotten until it happens again. Good security is when nothing bad happens, and when nothing bad happens, who needs security? Everybody hates the constraints of security and wants them to go away. CISOs have tried to justify spending resources on security by claiming that they can manage and reduce security risks by assessing, reporting, and controlling them. They try to measure

the benefits of information security “scientifically” based on risk reduction. This doesn’t work.

I claim that security based on risk management, risk reduction, and risk assessment is a failed concept. I am not alone in this claim. A majority of CISOs at a 2003 Gartner security conference also claimed that risk assessment is a failed method of making security decisions according to an article in *ComputerWorld*. I propose that intangible risk management and risk-based security must be replaced with practical, doable security management with the new objectives of due diligence, compliance consistency, and enablement.

The debate about security risk is obscured and confusing because supporters mix together risks and certainties that are not risks. To support my proposed replacement of risk-based security, we must have a clear understanding that security risk is the anticipated frequency of losses from intentional and accidental rare abuse, misuse, and natural loss events focusing on information. Computer viruses and worms are not risks; they are certainties since they are occurring with high frequency (probability of one). Events that occur only with material probability of less than one and greater than zero by definition are risks that would be amenable to estimation of frequencies. Ongoing events like virus and worm attacks are subject to security management through measurement and control by straightforward calculation of return on investment (ROI) or net present value (NPV) based on plenty of available valid data.

Also, security risk is quite different than business risk that consists of forecasting of investing resources to produce a profit. It also has no relationship to IT risk that forecasts probabilities that a new or changed system or application or development project will be financially successful. Investing in the reduction of security risk, on the other hand, results in some unknown possible reduction of loss that is not measurable since it hasn’t happened yet and is unknown. Methods for attempting to evaluate security risks are the emperor’s new clothes. In my experience many efforts to use such methods (e.g. NIST Annual Loss Expectancy) such as those recommended in three recent articles in *The ISSA Journal* have faded away when the high cost, easily disputable results, and changing environment are realized. Many small automated risk assessment businesses quickly fail.

It is not possible to know the effectiveness of safeguards that have no detection capabilities associated with them. Howard Schmidt stated (in *ComputerWorld*, September 26, 2005 at an ISACA Conference in Las Vegas) that: “...often you can measure a negative event but not a positive one. As a result, it becomes very difficult to demonstrate the business value of security programs.” Good security is when nothing bad happens, but with nothing bad happening, there is nothing to measure. Therefore, the goodness of security against rare incidents can’t be measured since you don’t know what you may have stopped.

It should be obvious to anybody familiar with computer and information misuse and abuse losses that information defenders can’t manage, assess, or control risks of rare incidents. The frequencies and impacts of future incidents are under the control of unknown and often irrational enemies with unknown skills, knowledge, resources, authority, motives, and objectives from unknown locations at unknown future times attacking known but untreated vulnerabilities and vulnerabilities that are known to the attackers but unknown to the defenders (a constant problem in our technologically complex environments). In addition, when enemies fail in attacking one possible vulnerability, they often attempt attacks on other vulnerabilities to accomplish their goals. Therefore, risks may be related in unknown complex ways so that reducing one risk may increase or

decrease other risks. This alone precludes the effective use of risk assessment methods.

The other factor in risk is impact. Impact, as part of risk, may be minimal in major attacks and major in limited or minor attacks. For example, remember the complete failure of Barings Bank in London resulting from a lack of segregation of duties in just one branch in Singapore. You never know what amount of liability, litigation, or secondary effects may ensue after even a minor incident. Also, there is no one-to-one relationship between one risk and one security effort since many security efforts may affect one risk and one security effort may affect many risks, which is occurring now with powerful security packages. Thus the impacts are related in unknown ways as well. The conclusion is easily seen to be that there are too many interrelated unknown variables and too many interrelated known variables with unknown values. And they all change in unknown ways over time depending on unknown future circumstances such as system changes, labor disputes, social and political changes, business changes, enemies’ plans and intent, and failures and successes and frailties on the part of enemies and defenders.

Risk-Based Security in GAISP

The ISSA Generally Accepted Information Security Principles (GAISP), v.3 is a work in progress that is an excellent expression of what information security is currently conceptually about. It shows dramatically that information security is conceptually incomplete, incorrect, and inconsistent. It is frightening that GAISP proponents are recommending that it be used to explain security to management. The current version of GAISP correctly assumes that the generally accepted concept of security is that it is driven by risk. But it fails to differentiate between manageable reduction of ongoing attacks that are certainties such as viruses and security risks of rare incidents.

In GAISP the pervasive principle of proportionality (2.5) is stated to be that: “Information security controls should be proportionate to the risks of modification, denial of use, or disclosure of the information.” Besides omitting several other sources of risks, GAISP contradicts itself in this principle by stating in the accompanying example, apparently in contradiction to pervasiveness, that: “Some organizations determine information security measures based on an examination of the risks, associated threats, vulnerabilities, loss exposure, and risk mitigation through cost/benefit analysis using a Risk Management Framework ... Other organizations implement information security measures based on a prudent assessment of “due care” (such as the use of reasonable safeguards based on the practices of similar organizations), resource limitations, and priorities.” Which is pervasive—risk-based as stated in the principle or care-based security stated in the example? How can risk-based security be pervasive if other organizations don’t accept risk-based security?

Unfortunately, security risk management has never been demonstrated to be valid. No study has ever been published to demonstrate the validity of information security risk assessment, measurement, and control based on real experience. And without assessment, security risk management is not possible. Therefore, information security as defined in GAISP is based on an unproven concept that is, in fact, not yet shown to be valid.

Fortunately, due diligence (or care) based on about forty years of information security experience along with compliance with regulations, legislation, and standards and enablement of business and government to meet their objectives have now become the defacto objectives in spite of all that is written about risk. However, these new objectives that are more important than the risk reduction objective still go unrecognized by many security experts and are not recognized as chief objectives in GAISP.

Intangible security risk reduction probably is being achieved serendipitously as a benefit of striving for the new objectives. This state of affairs is not recognized in GAISP. Compliance, due diligence, and enablement should replace or at least be given greater emphasis than risk reduction in GAISP. I realize that this will be very difficult to accomplish because unprovable, unmanageable, and intangible risk-based security is so ingrained in all that we do and say, but the time has come for change as standards, legislation, civil litigation, and Internet business competition forces due diligence, compliance, and enablement upon us.

Invalid Risk-Based Security in Practice

Supporters of security risk management and risk assessment in debates with me (CISSPs are referred to the risk threads in the CISSP Forum) often admit that so far, in the advance of information security, there is not enough valid data to make risk assessment a straightforward and successful method. However, they argue that this is not a reason to abandon it. They say that we must continue to strive to obtain the necessary valid data, and it will be possible to ultimately attain the goal. I suggest that with the increasing number of computer users worldwide, increasing dependency on growing numbers of computers, complexity of systems and networks, and advancing sophistication and effectiveness of criminal attacks, that there is no hope of ultimate success of risk management and assessment.

People such as Dan Geer, whose background is statistics, believes that the problem of insufficient data is researchable and solvable in about ten years in a statement that he made at the 2006 RSA Conference. In the meantime, he suggests that we should continue trying, expanding our databases and stick to a coarse granularity level of ordinals (estimating in terms of ones followed by lots of zeros). Others claim they can do it quantitatively now. These are CISOs who are strongly committed to risk-based security by having significant ongoing risk management functions, and job titles and descriptions that include risk management. Some of them explain that the numbers simply constitute a language to express opinions and intangibles that CISOs, business units, and top management understand to justify their decisions that they have already reached concerning their security requirements.

One CISO told me that he performs risk assessment backwards. He says that he already knows what he needs to do for the next five years to develop adequate security. So he creates some risk numbers that support his contention. Then he works backwards to create types of loss incidents, frequencies, and impacts that produce those numbers. He then refines the input and output to make it all seem plausible. I suggested that his efforts are unethical since his input data and calculations are all fake. He was offended and said that I didn't understand. The numbers are understood by top management to be a convenient way to express the CISO's expert opinion of security needs.

Supporters of risk-based security also point out that risk assessments are required in much recent legislation such as in GLBA and SOX. My inquiries about how CISOs go about performing risk assessments to meet the requirement lead me to conclude that regulatory requirements can be met by performing a "very high level" assessment that in a few paragraphs describes the dangers that a corporation is most concerned about with appropriate caveats that much is unknown. Some risk assessments now consist of prioritizing which applications, systems and networks are in most need of security attention because of their critical role in the business of the organization, especially in meeting the requirements of SOX.

Dave Cullinane at Washington Mutual on June 3, 2004 presented an ISSA Chapter talk on meeting the SOX requirements. With his approval I paraphrase from my notes as follows:

Risk assessment consists of identifying all applications in four levels of sensitivity relative to financial reporting and business records. The highest level consists of applications producing the final net value and performance of the bank. He found 85 applications at that level based on the advice of business managers. The other levels are for applications that feed into the next level. The lowest level consists of applications that process transactions and input data. New applications are being created throughout the bank continuously and represent an almost impossible challenge to keep up. He uses a due diligence approach and spends time visiting and communicating with other CISOs and using benchmarking to determine generally accepted practices that he must have. He does no formal quantification of frequency and impact of incidents, and he explains the security needs to management in terms of due diligence in meeting the requirements since SOX holds management responsible for the integrity and authenticity of the financial records.

With rapidly expanding regulations, risk is transforming from risk of rare incidents to risks of failure to meet the regulatory requirements and the impacts of penalties that might ensue. The Career Corner article by Jeff Combs in the November 2005 issue of *The ISSA Journal* defines risk management and gives examples of risks to be managed. They concern availability, performance, scalability, recoverability, human capital, and outsourcing. He doesn't include the risk of loss incidents such as fraud or theft.

"Security's Shaky State" in *InformationWeek*, Dec. 5, 2005 stated that their latest survey of 1522 responses from IT security administrators, managers, midlevel executives, and corporate executives indicates that IT security is underfunded, understaffed, and underrepresented. The top five drivers in that year's survey are improving business practices, auditing regulations, industry standards, security breaches from external sources [these are mostly certainties, not risks], and legislative regulations. The most pronounced shift from last year's survey is the increasing importance of compliance issues for assessing risk before information security purchases. Compliance hit the top spot as a risk assessment driver. CISOs must learn to "talk the talk" of compliance and move security from a technical control to a business control, and they don't see inside threats as their problem according to the article. The Computer Security Institute (CSI) Alert Newsletter for December 2005 in an article reporting on a panel of CISOs at the CSI 32nd annual conference generally agreed that regulatory compliance, particularly in regards to Sarbanes-Oxley, is still the major driver of security efforts, despite being a hindrance to more thoughtful, comprehensive security management.

Security Risk Assessment and Management

I suggest that the reason that top management underfunds, undersupports and underrepresents information security (as reported in the trade media and from complaints by CISOs) is because information security is represented to management as being based on intangible risk reduction that is easily refuted or ignored. Risk reduction is a weak justification for security.

Justifying increased support for security by reporting to management that a security risk is measured to be a certain value (quantitatively or qualitatively) is folly. Management's business is risk-taking, and when a secu-

rity risk is presented to them, they are able to respond that they take risks every day. And they simply accept the risk presented to them and refuse to support the security that is claimed to reduce it, especially when they see the negative impact and inconvenience that security has on the organization and their business goals. When the reputed risk doesn't materialize into a loss event, or some other larger unpredicted risk materializes instead, there is a justified loss of trust and belief in the value of security risk assessment and those presenting it. Also, management is generally intelligent and experienced enough to know that security people are likely to exaggerate their findings or resort to guessing to justify their recommendations. This remains to be proved, but I have seen examples of it in my own experience.

On the other hand, if we present to top management (as I have in many security reviews for clients) that they should support security for reasons of achieving due diligence, compliance, and enablement, they have little reason to resist (subject to various management cultures and business circumstances). I find that they are more likely to approve recommendations based on my experience and the following reasoning:

Due diligence: We can show management the results of our threat and vulnerability analysis (using examples and scenarios) by giving examples of the existence of the vulnerabilities and solutions that others have employed (not including estimated intangible probabilities and impacts). Then we can show them easily researched benchmark comparisons of the state of their security relative to other well-run enterprises and especially their competitors under similar circumstances. We then show them what would have to be done to adopt good practices and safeguards to assure that they are within the range of the other enterprises. This is based on 35 years of experience from the beginnings of information security of what others have done and from what is available from the multi-billion-dollar information security products and services industry. We also identify standards and well-accepted guides as the sources of good practices and safeguards. If management spurns any of our recommendations, we document this and the good business reasons for it to limit our and management's liability. The ultimate motive here is avoiding management negligence (and possibly litigation) to achieve due diligence and serendipitously possibly reduce risk as well.

Due diligence need not result in mediocrity and failure to advance security by using old solutions. Every organization does some security well and some security poorly. Due diligence takes the good that some do as a source of good practice and therefore spreads a higher level of security than would otherwise be obtained. New security for new technology comes from the research and development in the information security industry motivated by profits, competition, existence of loss experience, and meeting customer needs. Due diligence also need not be proven valid since the final results prove themselves from good or bad experience. And the results are direct solutions as different from risk assessment, where solutions don't come from assessment but must be chosen by due diligence and then tested again by further risk assessments.

Compliance: We are finding that the growing body of security compliance legislation such as SOX, GLBA, and HIPAA and the associated personal and corporate liability of managers is rapidly becoming a strong and dominant security motivation. The FTC has already demonstrated their intent to regulate by applying significant penalties in a number of cases. (The current legislation is poorly written and has a sledgehammer effect as written by unknowing legislative assistants but will probably improve with experience, as has computer crime legislation.)


Enablement: It is easily shown in products and services planning that security is required for obvious and competitive purposes and from case

studies, such as the Microsoft experience of being forced by market and government pressures to build security into their products after the fact.

I find that top management is relieved to not have to deal with quantitative and qualitative risk assessments that are easily subject to question. They more readily accept, sometimes with resignation, the recommendations and demands required of them by these new tangible and measurable objectives. This is especially the case when they hear the requirements from internal and external auditors and regulators as well (who are also held to account in the legislation) and recognize the personal and corporate liability involved.

Conclusion

The bottom line is that no matter how elaborate or "scientific" the risk assessment methodology is, whether it is Octave, FAIR, FRAP, or even Dr. Kevin Soo Hoo's that is the most complete mathematical model of risk assessment methods ever developed, there are no sufficiently valid frequency and impact data that will make the results valid. Business managers can guess the frequency and impact of a rare loss incident, but an event, circumstance, or enemy unknown to them can materially change the risk, making any security decisions or their implementations the wrong ones done in the wrong ways at the wrong times. And the situation will get worse because of increasing complexity and change of technology, opportunities for crime, numbers and types of enemies, and potential for loss.

There is only one solution available to us. Replace intangible and unmanageable risk-based information security with security management based on due diligence, compliance, and enablement. This can be accomplished without loss of face, integrity, or reputation by rejecting risk-based security articles in our trade and professional publications, perform only high-level general risk assessments when they are required, gradually eliminate risk assessment in our policies and practices, and emphasize and practice due diligence, compliance, and enablement. 

Donn B. Parker, CISSP, is a retired senior information security consultant at RedSiren Inc. (spun off from SRI International). He has specialized in information security and computer crime research for 35 of his 50 years in the computer field. He has written numerous books, papers, articles, and reports in his specialty based on interviews of more than 200 computer criminals and security reviews of 250 large corporations.