



Securities Industry Association

120 Broadway - 35 Fl. • New York, NY 10271-0080 • (212) 608-1500, Fax (212) 968-0703 • www.sia.com, info@sia.com

October 12, 2004

The Honorable Adam H. Putnam
Chairman
Corporate Information Security Working Group
Subcommittee on Technology, Information Policy, Intergovernmental
Relations and the Census
Government Reform Committee
U.S. House of Representatives
Attention: Clint Kreitner ckreitner@cisecurity.org

Re: Draft Report of the Best Practices and Metrics Teams

Dear Mr. Chairman:

The Information Security Subcommittee of the Technology Management Committee of the Securities Industry Association (“SIA”)¹ appreciates the opportunity to provide comments on the Draft Report of the Best Practices and Metrics Team of the Corporate Information Security Working Group (“CISWG”) (the “Report”). The Report is intended to help Board members, managers, and technical staff establish a comprehensive structure of principles, policies, processes, and performance metrics to support the people, process, and technology aspects of information security across a wide variety of organizations. The Report expands on previous work in which the CISWG created a list of Information Security Program Elements regarded as essential content for comprehensive enterprise management of information security.² We understand that comments were requested by October 6, 2004 and so we very much appreciate the added time you granted in order to allow us to comment on this important effort.

¹The Securities Industry Association, established in 1972 through the merger of the Association of Stock Exchange Firms and the Investment Banker's Association, brings together the shared interests of nearly 600 securities firms to accomplish common goals. SIA member-firms (including investment banks, broker-dealers, and mutual fund companies) are active in all U.S. and foreign markets and in all phases of corporate and public finance. According to the Bureau of Labor Statistics, the U.S. securities industry employs 790,600 individuals. Industry personnel manage the accounts of nearly 93-million investors directly and indirectly through corporate, thrift, and pension plans. In 2003, the industry generated \$213 billion in domestic revenue and an estimated \$283 billion in global revenues. (More information about SIA is available on its home page: www.sia.com.)

² See <http://reform.house.gov/TIPRC/>.

SIA believes the goal of developing a resource upon which a structure of actionable guidance could be built is a laudable one. However, in the current environment, regulated entities face an array of standards and guidelines relating to information security (*e.g.*, Gramm-Leach-Bliley Act, Regulation S-P, Sarbanes-Oxley Act, etc.). Ideally, the program elements and supporting metrics set out in the Report should complement existing regulatory requirements. Commonality will ensure that when the industry complies with one set of requirements, it will satisfy other requirements as well.

The Report acknowledges that the Information Security Program Elements and Supporting Metrics are not offered on a “one size fits all” basis. Recognizing the disparate needs of different organizations, the Report states that the suggested metrics are subject to modification and supplementation as desired. Despite this flexibility, we are concerned that the content and language of the Report could establish a new liability/negligence standard that is not appropriate for a particular industry or set of business operations. Therefore, we believe the Report should expressly state that the recommended elements and metrics are completely voluntary and the specific details are left to each individual institution to define in light of the specifics of their business and environment. Because each organization would have to conduct its own cost benefit analysis and decide on the applicability of the guidance contained in the document to its internal information security program, we question whether it will be immediately useful for the end user.

In addition, we question the usefulness of certain suggested metrics. A metric should be something that is easily understood and universally agreed upon. Many of the figures called for in the Report are statistics, not metrics. As discussed in more detail below, important terms are undefined leaving room for subjective interpretation. Given that many of the percentages are based on measures that are subject to interpretation, comparisons from one organization to another, or even from year to year within an organization, would be difficult. Additionally, the utility of percentages is questionable unless they are risk-weighted and prioritized, and can be compared to some industry standard. Moreover, depending on the interpretation, there are elements and metrics listed that address items that securities firms may not address today, *e.g.*, classification of information assets, role based access controls, etc., that may dictate a particular technology or system, which would limit our flexibility and discretion.

In fact, risk assessment, including operational risk, is critical in the securities industry but generally does not result in the establishment of measurable thresholds. Information security is integral to risk assessment and necessarily must be assessed as part of the overall business process. We would prefer if the Report focused more on the underlying operational risk process and the role of metrics within the process, and less on specific metrics that may or may not be particularly relevant. Security is an ongoing process, and metrics that are expressed as a percentage naturally lead organizations to achieve 100% as an obvious goal. Security is a risk that needs to be mitigated, but cannot be completely eliminated. However, because security is an ongoing process, a

company's 100% in one metric in a given year does not mean that the company is going to achieve 100% again, or that their 100% is comparable to another company's 100%. Many times, a company that achieves a lower percentage by concentrating on the issues that matter is more secure than a company that achieves a higher percentage by setting lower standards. Perhaps the most useful metrics in information security are those that are unreasonable for repeated achievement of 100%, such as password resets.

As drafted, the Report suggests that information security can exist independent of the business itself and can be applied to assets, programs, objectives, and functions independent of the business process. A more desirable approach, we believe, is one that directs the Board and management to include information security as part of the business process. For example, the process of establishing risk thresholds for critical information assets does not contribute to the ability to assess risk independent of a business process. It takes a reverse engineering process to determine where data is stored, whether it is replicated from another source, in what systems it may be processed, aggregated, fragmented, or consolidated before the risks can be assessed. Only after determining all the places within the information technology infrastructure that the information may be housed and transmitted can a Board member fully appreciate the type of reverse engineering process needed to devise a risk threshold calculation based on potential risk within the information technology infrastructure. Also, where regulatory requirements do not allow for flexibility, the acceptable risk threshold must be zero. Therefore, it would be more useful for Board members to concentrate on business processes that rely on information security.

Our comments on specific sections follow.

Information Security Program Elements and Supporting Metrics for Boards of Directors/Trustees

1. Important terms are undefined. Specifically, it is not clear what an "acceptable threshold" would be for purposes of establishing risk thresholds and who defines it. As noted above, in certain instances, the acceptable threshold must be zero. "Key information asset" is subject to interpretation. For example, a keyboard is an asset but so is a database. Other terms subject to interpretation include "comprehensive," "implemented," "objectives," "significant or material," and "functions."
2. Again, certain terms regarding establishing principles and assigning accountabilities should be defined (*i.e.*, "principles," "fully implemented," and "policies and controls"). Also, the use of percentages does not account for the degree of risk. If an organization establishes a Chief Information Security Officer ("CISO") role and assigns all the tasks to the CISO, should the organization achieve 100%? Also, it is not clear who would be "a responsible authority" for purposes of deeming employees to possess information security knowledge, skills, and certifications appropriate for their position. If, in fact, the employee is

deemed to have the requisite knowledge, skills, and certifications but is not primarily held accountable, use of such metrics will not adequately measure the degree of risk. Therefore, it should be within the judgment of management (who is accountable) as to whether any certifications are required. In many cases, it is best left up to the institution to determine the competence of their staff.

Alternatively, perhaps the metric is better phrased as “the percentage of employees with information security responsibilities that hold the information security credentials required by their job function as approved by the Board.”

Another useful ratio would be the percentage of all certifications in the Information Security department to the number of staff, which would demonstrate whether the department, on the whole, is well-certified or if certification is concentrated within a few individuals.

3. In connection with protecting stakeholder interests dependent on information security, “security incident” needs to be defined. The most egregious security incidents are those that go undetected. Consequently, a metric that relies only on detection is an ineffective protection measure because if a firm’s information security monitoring is limited, it may not even be apparent that a breach has taken place. This potentially penalizes firms with strong auditing tools that detect security incidents after-the-fact.

Also, “damage” can be measured in many ways. For example, for each virus that infects an organization, you could measure: the number of machines infected to the population of machines; the mean, median, and standard deviation of the above percentages; or the number of viruses that infects the organization to the number of known viruses that year. Damage is also commonly calculated as hard and soft dollar costs.

4. With respect to strategic partners and vendors, it is not clear why a straight percentage relating to information security requirements would be useful information. The Report should define a strategic partner and should indicate that an organization must determine if a non-strategic partner could introduce risk as well. In fact, often partners and vendors are monopolists or oligopolists that use their leverage over financial services firms to resist specific operational requirements for information security. They have no market incentive to be security-conscious. In addition, they attempt to disclaim legal liability in their contracts. Without corresponding liability, the information security requirements that securities firms can impose are relatively ineffective because the vendor or partner may not have sufficient legal incentive to comply. There also needs to be information security requirements or standards against which both customer and partners/vendors are measured.
5. It is not clear if “objective audit” contemplates use of a third party. The provision should be explicit. It should also recognize that an audit typically does not cover *everything* that the law requires.

6. Percentages do not provide useful information in relation to internal and external audits. An audit can be simple or complex. To achieve a high percentage, the Board can reduce the number of audits but make each more comprehensive, or increase the number of audits but make each more specific. Additionally, not all audit findings relate to critical resources; there should be some risk-weighting. It also is not easy to determine if an audit finding has been “corrected.” Often, a finding may involve a response, an amendment to a policy or procedure, or simply a new practice.
7. Information security metrics to be reported to the Board must be clear on what is reasonable, what they cover, and who sets them. Generally, we believe target values are problematic.

Information Security Program Elements and Supporting Metrics for Management

8. Regarding policies and controls, the total population is not clear. It could refer to the internal policies on a firm’s books or to some external set of policies and controls that the industry agrees is appropriate. 8.3 requires approval by senior management but monitoring by senior management and the Board of Directors. It is not clear how the Board would know to monitor the controls if they haven’t approved them.

The percentage of staff assigned responsibilities for information security policies who have acknowledged accountability for their responsibilities could simply mean that everyone signs such an acknowledgment as part of the employment contract, and does not reflect how well an organization is doing in terms of information security. Also, “violations” can be variously interpreted, especially in the interest of reducing the number to zero. Violations should be considered in terms of criticality, risk, etc.

9. At some level, all access to information systems is role-based so the definitions relating to information system access privileges must be clear and terms subject to varying interpretations should be defined (*e.g.*, “comply,” “access”). Again, percentages do not necessarily provide useful information.
10. With regard to assessing information risks and actively managing risk mitigation, it is important that the assessment be current; the language should be more explicit than “critical assets and functions” and should include systems, networks, processes, etc. “Defined” can be interpreted variously as well.
11. Percentages of known information security risks that are related to strategic partner or vendor relationships are not useful in assessing whether a company is doing well with respect to information security. Additionally, the percentage of strategic partner/vendor agreements that include external verification of policies

and procedures are only meaningful if an organization is going to verify that the partner/vendor is doing what is included in the agreement. Securities firms would want to retain some control and discretion in how they fashion vendor agreements and contracts in the area of information security and monitoring of vendors.

12. When identifying and classifying information assets, quantification should be limited to critical information.
13. 4 and 13.5 speak in terms of “attacks” but should refer to “events;” damaging events might occur as a result of unintentional activities.
14. The element that speaks to management responsibility to approve information systems architecture during acquisition, development, operations, and maintenance should distinguish between architecture and applications. The two are subject to different types of review. Also, what is “adequately mitigated” will depend on the level of risk. As noted with respect to other metrics, there should be prioritization and/or risk weighting when assessing whether identified security risks have been adequately mitigated.

SIA also believes that experience demonstrates that metrics represented as percentages will be viewed as a scorecard where 100% is the obvious goal. Not all metrics in the current draft are stated as objectives to be achieved, *e.g.*, “percentage of critical information assets or functions residing on systems that are currently out of compliance with the approved systems architecture.” If instead stated positively, the metrics could form the basis for a six-sigma-like effort within organizations to minimize defects. However, this approach should be cautiously applied because of the potential for a lone vulnerability to jeopardize the organization. For example, where a sub-business unit has one unapproved firewall rule allowing any Internet access, its connectivity with a larger business unit may be a .000003 defect in the larger business unit’s metric, positively stated as the number of firewall rules that are reviewed and approved. The seemingly insignificant control weakness could be exploited to negatively impact the entire organization.

15. The element regarding protecting the physical environment should refer to *critical* servers. In certain cases, physical risks may be insignificant unless the compromise of information assets and functions could affect critical resources.
16. As noted above, each organization must perform a cost benefit analysis before implementing the metrics outlined in the Report. Some of these metrics would involve full-scale consulting assignments, *e.g.*, percentage of information security requirements from applicable laws and regulations that are included in the internal/external audit program and schedule. It is difficult enough to find an internal or external auditor that can define coverage for “applicable laws and regulations.” To require them to measure whether they had done it is redundant

with their job function. To report below 100% would be cause for dismissal and to omit low-risk laws and regulations would result in a skewed metric that would not be meaningful. Alternatively, a management “overseer” could be responsible for the measurement, although such a project undertaken in addition to the audit itself could be prohibitively expensive and would not be likely to produce a more meaningful metric than the audit. With respect to the audit, the Report also should specify which laws and regulations (domestic *and* international?) are applicable and who makes that determination.

17. It is assumed that the information security metrics to be reported to management will be calculated by various units of the organization and aggregated at various levels up to the entire enterprise. We agree that metrics should be hierarchically structured and different level metrics are better managed at different management levels. The examples given in the Report, however, are a mixed bag and may not be useful or the best metrics to use for the specific organizational structure and processes.

Information Security Program Elements and Supporting Metrics—Technical

Because most of an organization’s information security policies will be implemented by assigning values to technical securities controls within the various information technology environments, risk assessment and criticality of systems are important considerations for this set of metrics. For example, with respect to user account management, there is a need to determine whether access is to sensitive data and critical applications and, if so, whether the administration of password safekeeping and the authorization of privileges are addressed. In connection with software change management, including patching, criticality of the system and urgency of the patch are important factors. If the threat level is low, there may be more risk inherent in applying the patch than in proceeding without it.

Conclusion

The degree to which an organization protects information against unauthorized access, disclosure, use, or damage is becoming more and more important. Increasingly, regulatory requirements govern information security programs. The securities industry is mindful of its regulatory obligations in this area and we urge CISWG to strive for consistency to the greatest extent possible with existing regulatory and legislative requirements. We have attempted to identify above those areas where specific guidance provided in the Report presents concerns for our industry. We appreciate the opportunity to comment on the Report and would be happy to address any questions you may have concerning our views. Please address questions to the undersigned or to Art Trager, Vice President & Managing Director, Technology, SIA, at 212.618.0546.

Sincerely,

Jennifer Bayuk, CISA, CISM
Managing Director, IT Security
Bear, Stearns & Co. Inc. and
Chairperson, SIA
Information Security Subcommittee of the
Technology Management Committee

cc: SIA Information Security Subcommittee
SIA Technology Management Committee
SIA Business Continuity Planning Committee
SIA Technology & Regulation Committee