



Security Evaluation Framework

Mark Egan
VP/CIO
Symantec Corporation
Megan@symantec.com



- Security Evaluation Framework
- Program Evaluation Examples
- Business Dependency Matrix
- Overall Program Assessment
- Summary

- Common question raised by CXO's on how is my information security program doing?
- Security lacks standard industry metrics such as earnings per share, on time performance, etc
- Security requirements vary considerably based upon company, industry, etc
- Security Evaluation Framework from my upcoming book (Executive Guide to Information Security - Prentice Hall) attempts to answer this question
- TechNet's Corporate Information Security Evaluation Guide for CEO's also leveraging this work

- Framework is based upon 50 industry best practices for information security
- Best practices are organized by people, process, and technology components of your program
- Business Dependency Matrix developed to provide weighted average scores based upon company and industry
- Grading is based upon score of 0-100 for evaluating security program
- Overall objectives; content rich, understandable by executives, inexpensive to use for high level assessment

Program Evaluation Template

Component	Score (0 -2)	Comments
Strategy <ul style="list-style-type: none"> • Written information security strategy • Strategy updated on regular basis • Proactive vs. reactive organization • Minimal impacts to business operations due to security issues • Industry compliance issues (eg HIPAA) have been addressed • Industry certifications (eg ISO 17799) have been achieved 		
Components <ul style="list-style-type: none"> • Qualified leader (eg CISSP) of organization • Experienced staff with necessary training • Dedicated information security staff • One staff per 1,000 employees • Ongoing training program in place 		
Administration <ul style="list-style-type: none"> • Function provides regular status reports to executive staff and board of directors • Executive staff own the Information Security program • Active engagement with critical functions such as Human Resources and Legal • Authority to enforce Information Security program • Segregation of duties • Performs risk analysis and management (assessments, audits, and compliance) 		
Total Score (0-34)		



Program Component	Score	Comments
People <ul style="list-style-type: none"> • Strategy • Components • Administration 	<hr/> 8 <hr/> 6 <hr/> 10 <hr/>	<ul style="list-style-type: none"> • No formal strategy exists today • Staff focused on day-to-day fire fighting • Informal responsibilities for Information Security • Minimal involvement of executive staff
People Score	24	
Process <ul style="list-style-type: none"> • Strategy • Components • Administration 	<hr/> 8 <hr/> 10 <hr/> 8 <hr/>	<ul style="list-style-type: none"> • Informal policies that are not followed consistently • Policies are not easily accessed by employees • All major security policies have been considered in program
Process Score	26	
Technology <ul style="list-style-type: none"> • Strategy • Components • Administration 	<hr/> 6 <hr/> 10 <hr/> 10 <hr/>	<ul style="list-style-type: none"> • No technology architecture in place and changes are very tactical in nature • Major technology components have been deployed • Informal program to protect environments from security threats
Technology Score	26	
Overall Average Rating (0-100)	76	



Component	Ratings (High - 3, Medium - 2, Low - 1)
Company Characteristics	
<ul style="list-style-type: none"> • Dependence upon systems to offer products and services to customers 	
<ul style="list-style-type: none"> • Value of company's intellectual property stored in electronic form 	
<ul style="list-style-type: none"> • Requirement for 24x7 business systems 	
<ul style="list-style-type: none"> • Degree of change within company (expansions, M&A, new markets) 	
<ul style="list-style-type: none"> • Business size (number of offices, number of customers, level of revenue) and complexity (processes, systems, products) 	
Industry Characteristics	
<ul style="list-style-type: none"> • Budget for security administration and security initiatives 	
<ul style="list-style-type: none"> • Potential impact to national or critical infrastructure 	
<ul style="list-style-type: none"> • Customer sensitivity to security and privacy 	
<ul style="list-style-type: none"> • Level of industry regulation regarding security (GLBA, HIPAA) 	
<ul style="list-style-type: none"> • Brand or revenue impact of security incident 	
<ul style="list-style-type: none"> • Extent of business operations dependent upon third parties (partners, suppliers) 	
<ul style="list-style-type: none"> • Customers ability to quickly switch vendors based upon their ability to offer services in a secure manner 	
Average Overall Ranking (Total Scores/12)	



Business Dependency	Program Rating	Overall Assessment
High	95-100	Good
	90-94	Average
	Below 90	Poor
Medium	90-100	Good
	80-89	Average
	Below 80	Poor
Low	85-100	Good
	70-84	Average
	Below 70	Poor

- Information security is not going to get any easier and comprehensive program required to address business requirements
- Key elements of the program include people, process, and technology
- Evaluation of your existing program is only the first step towards improvements