Global Information Assurance Certification Paper

Creating a monthly Information Security Scorecard for CIO and CFO

GIAC (GSLC) Gold Certification

Author: Michael Hoehl, mmhoehl@gmail.com
Advisor: Kees Leune

Accepted: December 24, 2010

Abstract

Executives are increasingly interested in the state of information security for their organization. The media and press are frequently reporting new methods of technology attack and how another organization has become a victim. Regulators and auditors including PCI, GLBA, SOX, HIPAA, etc. are demanding more executive time and attention. Routinely communicating in a clear and concise manner with the CIO and CFO is necessary for today's information security leader. Determining what should be communicated and in what format can be a challenge. This paper will provide readers an approach for creating a Security Scorecard to routinely update the CFO and CIO regarding information security compliance, investment, and risk metrics.

1. Introduction

Identifying the specific security metrics desired by executives ultimately accountable for information security financials and organization risk management is a daunting task. Common security metrics report how well policies, processes, or controls are functioning. Though this operational perspective is important, additional insight may be desired to reveal the capability maturity of the organization's security practice (right way), assure I.T. investments are being made based on risk management (right amount and order), and confirm the organization's business objectives are being advanced (right outcome).

As stated in the Corporate Information Security Working Group Report of the Best Practices and Metrics Teams (2005) , "Metrics are about transforming policy into action and measuring performance" (p. 5). Security policies are necessary to reinforce business objectives, and establish requirements necessary to advance these objectives. However, policies without metrics are like trust without a history of accountability. Metrics provide transparency into an organization by measuring the adoption of the policies and how effective the current policies are at achieving the desired outcomes.

Metrics must be clear, concise, and compelling to avoid the "so what?" response from executives. What may seem obvious and intuitive to the security professional may not be so for today's business executive. Further, these metrics must be delivered in a recurring and sustainable manner to remain relevant to the executive. This can be a big challenge for security leaders that must juggle security infrastructure management, security incident handling, compliance reporting, and internal auditing roles. Only a finite amount of time is available to report relevant information to executives while at the same time managing other security duties.

Getting started with gathering and publishing security metrics to executives can be a challenge. In the March 2010 article "Proving Your Worth " in Security Information Magazine (p. 29), Andrew Jaquith of Forrester Research identifies 3 major pitfalls of security metrics program development: enterprises try to measure everything; convenient

metrics are selected rather than meaningful ones; and data lacks contextual relevance. So how can these pitfalls be avoided?

Unfortunately, there is no ubiquitous or authoritative metrics reference containing all data relevant to all organizations. Business objectives are typically unique to each organization—so messages and metrics must vary based on these objectives. A versatile framework solution is needed that can be applied to each unique organization dynamic. Information technology leaders need a "scorecard" to measure performance and help transform policy into practice.

This paper provides an approach and framework that the security professional can follow to make a Security Scorecard for Executives. Guidance includes revealing the metrics Executives are interested in, determining which security metrics should be gathered and presented, identifying who should be involved, finding available references, and approach creating a recurring Security Scorecard. The Security Scorecard will then become a valuable tool for routine and sustainable executive communication.

2. Why would a CFO or CIO want to see a Scorecard?

2.1. Decision Support

Executives including the CEO, CFO, COO, and CIO are accustomed to numeric information including annual operating plans, department budgets, P&L, inventory, supply chain management, and sales forecasts. They review many of these complex reports daily. The reports containing this information must satisfy the executive's need for clear and credible data that drives decision making. A popular report for executives is the business "scorecard". Scorecards are used for strategic decision support—especially for financials and operations. For business decision support, scorecards are created to present brief answers to the following questions:

- Are we meeting our fiduciary requirements?
- How do we compare to our peers?
- Are we advancing our objectives?
- How are we identifying and managing risk?
- Are we improving?
- Are we investing in and advancing initiatives in the right order?

Executives are asking for security metrics with more visibility into organizational risk The Security Scorecard is intended to provide the vital security information that reveals how the organization is performing and drive decision making.

2.2. Peer Pressure and the Press

Executive interest in security can be driven by communication within the organization or by trusted peers outside the organization. The media and press are frequently reporting new methods of technology attack and how another organization has become a victim. These reports generally include statements from executives having to account for the security breach or institutional misconduct. This is causing growing concern for many executives. Regulators and auditors associated with PCI, GLBA, SOX, and HIPAA are demanding more executive time and attention regarding security. Internal staff are exploring new ways to conduct business and reach out to customers—and security seems to always be a concern. Organizations are collecting and presenting increasing amounts of data that must be safeguarded. Executives want to have greater insight into their organization's information security status—especially as it applies to achieving business objectives and organization mission.

2.3. Elevator Meetings

One of the most critical reasons for getting a Security Scorecard in the hands of the executive is as a speaking aid for the executive when they socialize the topics discussed during the recurring security meetings. Since the executive may not be comfortable with all the "security speak", expect that the Security Scorecard will be used as speaker's notes while talking to fellow executives within and outside the organization.

Further, the Security Scorecard will be used as evidentiary support for the executive's call to action. If asked "How is it going with information security?", the Security Scorecard should provide credible summary data to support advancing investment of business resources. Don't discount the effectiveness of the follow-up executive conversations and the potential interest this document will foster. The executive will forward Security Scorecard information as a follow-up to formal meetings

or even an impromptu meeting with peers such as an elevator conversation or possibly a golf outing. This will help to further promote the security initiatives in a credible manner.

2.4. Transparency

Finally, executives and officers of organizations have a growing interest in the governance, risk, and compliance (GRC) associated with information technology. Security is accountable to all three of these areas. Fear, uncertainty, and doubt are no longer credible arguments for justifying current expense levels or requesting additional capital investment. Transparency is being demanded to reveal that the organization is making the right IT investments, at the right time, with the right resources, and in the right way. The Security Scorecard provides information at the executive's fingertips with clear, concise, and actionable data that reinforces the value of current and proposed investments.

3. What Security Metrics would a CFO or CIO want in the Scorecard?

3.1. Identify business objectives

One of the biggest challenges for a security professional is to understand how security relates to the business executive's mission. This is the first step—and is many times the most difficult. What is intrinsically obvious to a security professional is not necessarily clear to a business professional. On the flip side, there are many complex concepts familiar to business professionals that may not be clear to a security professional. As a test, just ask a security professional to explain their organization's year end financial report. They have a better chance of explaining EBCDIC than EBITDA. If the security professional does not understand how security relates to the organization from a business executive perspective, then they will not be able to take the first step in answering "Why is security relevant to the business executive?" Answering this fundamental question will require investigation by the security professional into the organization's business objectives.

3.1.1. Helpful Tips to find Business Objectives and Fiduciary Obligations

Resources that identify main business objectives (MBOs) include quarterly statements, the corporate Intranet website, employee communications, and CEO letters. In some cases, the security professional's own performance plan may include text that references the organization's or department's major objectives. Executive assistants are a great resource to quickly obtain a copy of the major business objectives—typically they helped the executives with the format and content of the presentation.

Several business units can be very helpful sources of information about the organization's objectives and risk concerns. The Finance department can be a source of guidance to find fiduciary obligations. Regulatory requirements including Sarbanes-Oxley (SOX) Act, Gramm-Leach-Bliley (GLBA) Act, Payment Card Industry (PCI) Data Security Standard, and U.S. state requirements all have security elements that the Finance leadership is concerned with. Human Resources has accountability for Health Insurance

Portability and Accountability Act (HIPAA). Legal has accountability for breach notification laws (e.g., California SB1386). Education organizations are accountable to Family Education Rights and Privacy Act (FERPA). The Electrical Industry has North America Electric Reliability Council (NERC) Critical Infrastructure Protection (CIP) standards. U.S. Government agencies have accountability to Federal Information Security Management Act (FISMA).

3.2. Consider Business Competitors and Authoritative Benchmarks

Most executives are competitive by nature. They are keenly aware of their organization's relative position to other companies targeting the same customer as well as the organization's perceived quality standard in the market place. Whether the benchmark is competitive or authoritative, the motivation is the same—being the best.

Several credible standards (e.g., Payment Card Industry Data Security Standard) and advisory institutions (e.g., Gartner, Forrester, SANS, etc.) organizations provide insightful information about how business competitors have adopted security. For example, the PCI DSS standard provides prescriptive guidance for retail organizations to properly safeguard credit card data. According to the Visa U.S. PCI DSS Compliance Status report (2010), "Over 96% of Level 1 Merchant organizations and over 95% of Level 2 Merchant organizations in U.S. are PCI DSS compliant validated." This is a compelling argument for a small to medium sized retailer to adopt the security controls associated with the PCI DSS 1.2. A Security Scorecard could use this information to report sustained (non)compliance with the PCI DSS 1.2 standard, and demonstrate how current compliance levels compare to similar merchants.

In some cases, the management teams that report to the executives are competitive with one another. The best example of this would be sales teams striving to reach goal first. Consider metrics presented by organizational unit or region. This will foster competition between the internal teams. Further, problems will be clearly revealed as systemic (correction is required across the whole organization) or atypical (targeted correction is required). Establish an organizational baseline, and then compare the different business divisions to this baseline.

Executives will also attempt to exceed the accepted standard of quality or normal commercial practices as a way to differentiate the organization. In this case the "competition" is actually a recognized authoritative standard—not an organizational peer. The executive may be intending to establish the organization as the "gold standard" in the market place. Research should be done to identify these peers and benchmarks. For example, manufacturers strive for ISO 9001 certification to demonstrate that formalized business processes are in place for quality management. ISO also has the 27001 certification for Information Security Management System. Several service providers pursue SAS70 certification from the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). If achieving and maintaining these recognized standards of excellence is a business objective, consider reporting current compliance status and risks to continued compliance.

3.3. Discover the Power of "Asking for Guidance"

Sometimes, the best way to determine an executive's interest in security is to simply ask. A brief interview can be quite revealing in determining what risk and security related concerns are on the executive's mind. The organization may be highly regulated and compliance concerns may be of highest priority. In other cases, risk avoidance is of highest concern. The organization brand or reputation may be the primary influence for decision-making. A recent security incident may be a serious concern. The incident may be internal—or even with a peer organization that was recently in the news. Even a recent audit could be motivating the executive to want more insight into security. The executive interview approach can identify risks that in turn reveal the metrics to consider for the Security Scorecard.

If the executive interview approach is taken to help formulate the contents of the Security Scorecard, be sure to come prepared. An ice breaker opening can be, "What is keeping you up at night?" Have a list of prepared questions to foster conversation to identify current organizational risks that have the attention of the executive. Bring a copy of the business objectives and examples of security metrics that are relevant to each objective. Ask the executive about the business metrics that are in place today, and ask how they provide value with advancing the business objectives. Be ready for a working

session if the executive is "hands-on" with creating the Security Scorecard content. This approach can be very helpful as it may not only reveal what is important to the executive, but also the presentation format the executive prefers.

Lastly, this approach helps avoid the "So what?" dilemma security professionals are sometimes confronted with when presenting data to executives. One of the best ways to ensure the Security Scorecard is relevant is to simply ask the executive what is important to the business. This question typically leads to a discussion about the business objectives and guidance on what "vital statistics" the executive leadership team is expecting from Security. If given this opportunity, identify current organizational risks that have the attention of the executive and determine if Security is an influencer. Though this iterative approach may take more time to generate a final product, the executive is essentially co-authoring the Security Scorecard in a way that is relevant to the intended audience.

3.4. Find risks identified in recent Audits

Auditors are the agents of executive management. Their role is to answer the question, "how do you know?" Implicitly, this means the audit had to start with asking what the executive and organization wanted to know. An audit report that identifies areas of risk or non-compliance can be very unsettling for today's executive. Some executives perceive a failed audit as an indication that their expectations of organization risk are incorrect. Worse, a failed audit can have a direct impact to executives including personal liability, lower compensation, and potential termination. These all can keep an executive up at night.

Audit results provide great insight into what is important for the organization to improve and sustain. A brief meeting with Internal Audit is another great way to fast track discovery efforts. Insight into recurring problems, current concerns, and near horizon requirements can be gained in less than an hour meeting. This research is also valuable for providing compelling arguments to track certain key performance indicators—as well as the risk of not tracking these vitals.

4. Which Security Metrics should be gathered and presented in the Scorecard?

4.1. Governance, Management, or Operational Metrics?

Essentially all Information Security programs are made up of three general areas: Governance, Management, and Operational. All three are necessary for a comprehensive information security program, however the metrics for each area are not for all audiences. In some organizations all three areas can be presented on a single scorecard. For other organizations, including all three areas in the scorecard may be confusing.

When creating a Security Scorecard, consider the audience. There may be multiple audiences with distinct perspectives and interests. Identify which elements are relevant to the each target audience to determine Scorecard content. Though every audience may share the same organizational business objectives, their role in achieving these objects will vary. Therefore relevant metrics will vary depending on the reader's role. Lance Hayden (2010) recommends, "It is more important that you know what you are trying to accomplish and let this drive your measurement efforts than to let the metrics decide this for you." (*IT Security Metrics : A Practical Framework for Measuring Security & Protecting Data* p.36). If your purpose is to motivate executives to continue to invest in the security program based on the current return on the investment, then a Security Scorecard based on governance information may be most valuable. The Security Scorecard should then provide clear answers to questions like: "Is the organization making the right amount of investment in security?"; or "Is the organization making security investments in the right order?"; or "Is the organization making security investments at the right time?; or "Is the organization getting the expected return on security investment?"

If the target audience's interest is ensuring quality control and primary motivation is continuous process improvement, then management related metrics would be most relevant. In this case, the Security Scorecard should answer questions like:"Is compliance improving compared to last year?"; or "How effective is the delivery of security awareness training?"; or "Are service level agreements in place for all managed security service providers?"; or "Are changes being made to critical systems without

proper authorization by the Change Advisory Board?"; or "What systems do not have an accreditation and certification program?"

Lastly, if your audience is technical and operationally focused, they will have a keen interest in the specific state of critical security controls. The Security Scorecard should answer questions like: "How many systems have configurations that deviate from standard?"; or "What recurring configuration vulnerabilities have been identified?"; or "What percentage of systems are logging security events in accordance to organization policy?"; or "What number of computers are not in a ready state for software or security updates?"; or "What are the number of security incidents over the last quarter?"

Knowing the questions that are most relevant to the intended audience will provide guidance into selecting content for the Security Scorecard. If there are multiple audiences with distinct perspectives, don't just provide a technical report with an opening executive overview. Clearly organize the Security Scorecard into governance, management, and operational categories. This way the reader can quickly recognize the information in the Security Scorecard relevant to their role.

4.2. Highlight Actions for Improvement not History of Failure

In *The Book of Risk*, Borge states "The purpose of risk management is to improve the future, not to explain the past." In *Security Metrics : Replacing Fear, Uncertainty, and Doubt* by Andrew Jaquith, the forward by Daniel E. Geer, Jr. quotes this same statement. This is a very important philosophy that scorecard authors should keep in mind. Occasionally being reminded of approaches that have failed in the past is an important "lessons learned" quality control—however frequent reporting of the same control failures without a clear call to action does not promote effective risk management.

For example, metrics reporting non-compliance for security updates is not relevant until the source of the compliance issue is revealed and necessary correction actionable. If general non-compliance is attributed to a specific department, system type, or software version, then this must be clearly presented by the scorecard. Risk mitigation begins with identifying what is causing or can potentially cause harm.

4.3. Concise and Actionable are the keys to success!

The Security Scorecard will be one of many reports on the executive's desk, so the Security Scorecard must be concise and actionable. Concise does *not* mean simple. Remember, the executives are running the organization—so they are capable of understanding complex organizational dynamics and consuming the necessary decision support data.

Actionable means the executive can see how their involvement is valuable in ensuring a desired outcome. General attribute data does not provide the executive any mandate to get involved. To be relative, the information must be related to a recognized and credible point of reference. For example, if the organization has an absolute patch compliance of 91.7%, the executive will not find this very valuable. If on the other hand a specific division of the company has fallen to 83.9% (or worse, competitors in the same market space average 95% compliance)--then the executive will want to know why the anomaly and will ask who should be engaged to correct this problem. Security Scorecards are similar to baseball scorecards in that they must easily relate the performance of 2 organizations or with an authoritative benchmark.

More metrics do not make Security Scorecards better. Many things that can be measured are not necessarily meaningful. Too much information in a Security Scorecard can delude important messages about risk or unintentionally convey a message of crisis. If the metrics do not advance the objectives of the business or represent a material risk to the organization, then they are not appropriate for the Security Scorecard.

Executives will accept relevant information in raw format—but they will not find value with irrelevant data in a fancy format. Metrics are not valuable simply because the data is visual and in a simple dashboard like format. Further, executives and management will request recurring progress reports to confirm that their intervention is producing the desired outcome. Security scorecards are intended to be updated frequently. Avoid creating complex scorecards that are resource intensive and not sustainable for monthly or quarterly updates.

5. Who should be involved with creating the Security Scorecard?

5.1. Identify the entire security team

Most organizations do not have a dedicated team of professionals with the collective responsibility for the entire security program. In many cases, the security program is effective because of the collaborative efforts of many teams with Security including PC support, database managers, application developers, system and network administration. Since these teams are critical to sustaining the security program, they are also critical to sustaining the Security Scorecard.

The Security Scorecard contains performance information about the security controls these teams manage. For this reason, these teams must be engaged early as part of the Security Scorecard development and continuously as the Security Scorecard is revised. This will ensure that there is one common and consistent message to executives. Most importantly, this approach will foster advocacy instead of conflict.

5.2. Create a RACI Document

Establishing roles and responsibilities in this environment is a critical first step when developing a Security Scorecard. Organization charts are typically too high level and not descriptive enough. A RACI document is a very valuable tool to document this understanding as well as identify gaps in duty assignments. This document is a matrix used to clarifying roles and responsibilities for cross-functional/departmental security duties. Project Managers use this tool frequently when leading a multi-team initiative. There are a few variations of RACI, but all have in common (R)esponsible, (A)ccountable, (C)onsult, and (I)nform.

The RACI is used in 3 different phases of the Security Scorecard. Initially during scorecard development, the RACI establishes collective understanding of who is ultimately responsible for each security control and who is performing the daily duties to ensure the appropriate state of the control. Advisors, auditors, and secondary support staff roles can are also be identified as part of drafting a RACI.

The second phase where the RACI is valuable is to determine the individuals that are the source of data for the Security Scorecard. To ensure that the Security Scorecard data can be updated routinely and credibly, resource planning will be required. The RACI will foster discussion about the people, process, and technology necessary to produce the necessary data for the Security Scorecard in a sustainable and unintrusive manner. Remember that without the information captured in a RACI document, it is very difficult to create manageable, repeatable, and timely Security Scorecards.

For the last phase (recognition), the RACI is used to help identify the folks that are accountable and responsible for sustaining the security controls. It provides a convenient way to put names to roles so that "job well done" messages can be personalized.

5.3. Don't forget Sponsors!

There is one other role that should be involved in the Security Scorecard, but unfortunately this role is not called out as part of RACI. The sponsor of each security control should also be included. The sponsor is typically a cost center manager or executive that provided the funding for the security control. In many cases, these individuals put some of their own professional credibility on the line to advance the funding and implementation of a security control. They can also be advocates for future investments.

The sponsors are also typically the advocate of the business and serve as proxy for "beneficiaries" of security controls. They are in touch with the current business priorities, current initiatives, risk appetite, and financial status. The Security Scorecard is a great way to communicate back to the sponsor the status and benefits of the security investments.

6. Where are helpful resources to further assist with creating a Security Scorecard?

6.1. Research On-line and Textbook Publications

There are few prescriptive documents and resources available for developing a Security Scorecard. There are, however, on-line resources from very credible authoritative sources that can help with brainstorming content for the Security Scorecard.

The National Institute of Standards and Technology (NIST) provides a wealth of information about technology, measurements and standards. The Special Publishing 800 series (e.g., SP 800-55 *Performance Measurement Guide for Information Security* and SP 800-33 *Risk Management Guide for information Technology Systems*) provide guidance for Information Technology professionals. NIST 800-55 proposes an approach with three measurable aspects of information security--business impact, efficiency/effectiveness, and implementation. NIST provides additional guidance with Interagency Reports (e.g., IR 7564 *Directions in Security Metrics Research* and IR 7358 *Program Review for Information Security Management Assistance)*.

The Center for Internet Security (CIS) has published *Consensus Metric Definitions* which provides twenty (20) metric definitions for six business functions: Incident Management, Vulnerability Management, Patch Management, Application Security, Configuration Management, and Financial Metrics. This is very helpful for establishing a common vocabulary of terms so that everyone is on the same page with regards to Security Scorecard metric meaning and maintenance.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) have collaborated to create the ISO 27000 series of guidelines for building an Information Security Management System (ISMS). Included in this series is ISO 27004 *Information Technology – Security Techniques - Information Security Management – Measurement*. Recently published in 2009, this document is expected to be adopted broadly as the authoritative source to assess security control performance and effectiveness based on ISO 27001. This document provides comprehensive guidance about the appropriate manner to collect, compute, and report Information Security Management System (ISMS) performance, however it does not

provide guidance to organizations for selecting which measurements and indicators are most appropriate and applicable based on business objectives.

The Corporate Information Security Working Group Report of the Best Practices and Metrics Teams provides guidance to get started with information security program elements and associated metrics for each general area. This is a great resource to help relate the appropriate type of data with the Security Scorecard target audience. .

Below are additional websites and on-line resources that can be helpful:

www.datalossdb.org.

www.securitymetrics.org

www.securityfocus.com

www.sans.org

www.isaca.org

www.cert.org

Andrew Jaquith has authored multiple books and articles on Security Metrics. His book *Security Metrics : Replacing fear, uncertainty, and doubt*. Upper Saddle River, NJ : Addison-Wesley, is a popular reference and emphasizes the importance of quantitative measurement as compared to qualitative measurement. Dennis Opacki*'s* work *Security Metrics: Building Business Unit Scorecards*, is helpful when considering a top down or bottom up approach to creating Security Scorecard content.. *IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data.* New York : McGraw Hill by Lance Hayden advocates Victor Basili's "Goal-Question-Metric (GQM)" empirical software engineering method for developing credible security metrics.

6.2. Consider Business Communication and Process Best Practices

Self-assessment and continuous process improvement are a common characteristic of any successful organization. As with all process reengineering and risk management initiatives, the Security Scorecard requires credible metrics. When choosing performance metrics, there is a broadly accepted approach abbreviated as SMART ("Specific", "Measurable", "Actionable", "Relevant", and "Timely"). "Specific" requires

that metrics be of a certain scope and targeted. "Measurable" requires that the data be of a quantitative nature that is easily verified and complete. “Actionable" requires that metrics clearly reveal the corrective action that needs to occur. "Relevant" requires that the metrics all have contextual value—that they are meaningful to the audience. "Timely" metrics require data be collected in a credible and repeatable manner that can be trended. Operational Excellence, Performance Management, and Business Process Reengineering all make references to SMART to ensure the right metrics are selected to achieve objectives.

Process maturity is also a key measurement of business processes. Executives and management use this data to determine current capabilities and to map out organizational plans to achieve the desired level of performance. Several capability maturity models exist including International Systems Security Engineering Association’s Systems Security Engineering Capability Maturity Model (SSE-CMM) and Carnegie-Mellon Software Engineering Institute (SEI) Capability Maturity Model Integration (CMMI) . They all offer a common framework that relates metrics and process management for information technology. Further, these capability maturity models provide measurement criteria and baselines for appraisal. After the Security Scorecard reveals what the control state is, the capability maturity models are useful in explaining why and what has to be done from a process perspective to achieve and sustain objectives. For example, the process maturity perspective can be valuable when investigating relations between enterprise software deployment services and system security compliance issues. As Lance Hayden states (2010) in “IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data, “Security is a business process” (p21). If you are not measuring and controlling the process, you are not measuring and controlling security.”

6.3. Review Relevant Legislation and Contracts

There are a number of regulatory and legislated requirements that organizations must comply with. For example, merchants accepting credit cards for payment must comply with PCI DSS. Organizations that maintain personal health information must

comply with HIPAA and HiTech. Corporations with publicly traded stock must comply with Sarbanes Oxley for financial governance and reporting.

Below is a short list of regulatory and legislated requirements that may be valuable for compliance reporting with the Security Scorecard:

EU Privacy Directive (Directive 95/46/EC)
http://ec.europa.eu/justice/policies/privacy/index_en.htm

FERPA (Family Educational Rights and Privacy Act)
http://www.ed.gov/offices/OM/fpco/ferpa/index.html

GLB (Gramm-Leach-Bliley) Act
http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

HIPAA (Health Insurance Portability and Accountability Act)
http://www.hhs.gov/ocr/hipaa/

HSA (Homeland Security Act)
http://www.dhs.gov/xabout/laws/law_regulation_rule_0011.shtm

NERC CIP (North America Electric Reliability Council Critical Infrastructure Protection)
http://www.nerc.com/page.php?cid=2%7C20

PCI (Personal Credit Information/Industry)
https://www.pcisecuritystandards.org/

SOX (Sarbanes-Oxley Act of 2002)
http://www.gpo.gov/fdsys/pkg/PLAW-107publ204/content-detail.html

Keep in mind that organizations may have additional legal obligations that are contracted—not legislated. Examples include customer contracts, vendor contracts, and service provider contracts. These contracts should also be reviewed to determine if they have requirements to monitor and report on the state of security controls.

7. How to create a Security Scorecard (recipes may vary!)

Just like there are many different recipes for bread, the metric content of the Security Scorecard can vary based on organizational "taste". This section provides an approach to creating a sustainable Security Scorecard. A variation of the Systems Development Life Cycle (SDLC) is adopted to plan, create, and control Security

Scorecard content. The SDLC approach also reinforces the cyclical nature of continuous improvement necessary for the Security Scorecard.

7.1. Prepare

The popular phrase "proper preparation prevents poor performance" applies to security performance reporting, too. To properly prepare requires a clear definition of scope and objectives. Many KPI and scorecard initiatives failed because of a lack of initial focus on what is to be accomplished or an expectation that everything must be measured initially. Do not attempt to measure all security controls right out of the gate. The Security Scorecard will evolve over time—as will scope. Research into major organizational and business unit objectives is a key to success. Define the initial scope to align with current organizational interest and business priorities.

Formally establish the target audience and stakeholders for the Security Scorecard. Investigate what is motivational to this audience. Don't forget to consider influencers, project sponsor(s), and recent security control investors (e.g., business unit leaders and IT management).

A formal project plan and charter documents lend credibility to creating a Security Scorecard. A project plan can be especially useful when coordinating multiple resources to assist in the gathering of Security Scorecard data. The project plan is not simply an activity list. At this phase the project plan should be a high level work breakdown structure that identifies major milestones and deliverables. Present charter documents to the CIO or project sponsor for formal commitment. A letter of authorization from the CIO is one of the most effective ways to get IT Management commitment.

Schedule a project kick-off meeting to present the initial project charter documents. Key resources and their management should be invited. Ideally, the CIO or sponsor should call the meeting. The Security Scorecard project gets instant credibility and is implicitly assigned a high level of authority by having the CIO send the meeting invitation and do introductions. Presentation material should map project objectives to key business objectives. The meeting should be brief with the attendees leaving with a

clear understanding of the project charter and their role. Finalize the meeting with next steps for team communication.

7.2. Analyze

A great follow-up to the project kick-off meeting is to conduct the Executive Interviews. This serves two purposes. The first purpose is to revisit the project objectives and confirm understanding. Review of the project kick-off meeting presentation material and a copy of the project charter is helpful. Don't assume this will be at the executive's fingertips for the one-on-one executive meeting. The second purpose is to gather information about the executive and their team. Prepare for these meetings with questions that will foster discussion about current organizational risks that have the attention of the executive. Ask for examples of current business KPI and scorecards the executive receives or references that can guide in the creation of the Security Scorecard. Present an early draft of the RACI. This will ensure the executive understands the purpose of the document and the value it offers.

Map security controls associated with mitigation of key risks identified by executives. Using the aforementioned RACI document, begin to identify roles and resources that manage the security controls. During this phase, research benchmarks and authoritative sources for the proper management of the security controls.

Review relevant regulation and contract obligations. Review recent audit reports and recommendations associated with these obligations. This includes general controls audits, regulatory compliance audits, and risk assessments. Request reports on the state of general IT security controls (e.g., patch and vulnerability management, malware prevention, web application security testing, etc.).

7.3. Design

In this phase, identify the key security controls that will be targeted for reporting in the Security Scorecard. Remember that the security controls selected to monitor and the metrics selected must provide clear indication that the objectives are or are not on track. If the metrics cannot be easily related to objectives or the metrics do not clearly

reveal progress (positive or negative) achieving objectives, then the Security Scorecard is not relevant.

The Security Scorecard may have an audience with various perspectives. Identifying these perspectives early helps with organizing the presentation of the data. Begin to group the metrics based on the business objectives when possible. This way the reader can follow the Security Scorecard based on their own objectives and interests. In some cases this may mean further grouping the data by Governance, Management and Technology. Help the reader of the Security Scorecard see their own reflection quickly so they can identify the risks (and call to action) that apply to them specifically.

Establish performance targets for security controls based on organizational risk appetite. For example, IT may have a service delivery target of 90% of computers eligible for a critical security update will have the update installed or vulnerability mitigated within 30 days. Using the RACI document, socialize these targets and performance goals to get consensus that these are in scope for the project and relevant.

Clearly define the metrics and how they should be interpreted consistently. This is a critical effort. If the metrics are ambiguous and the call to action unclear, then the Security Scorecard will lose credibility. Below is an excellent example from Job Asheri Chaula, Louise Yngström, and Stewart Kowalski, Department of Computer and Systems Sciences, Stockholm University/KTH, "Security Metrics and Evaluation of Information Systems Security" (p. 10) demonstrating how a metric should be documented.

Testing Goal	To determine if there sufficient documentation explaining how IT systems has been installed.
Associated question	Is there any policy document?
Metric	Percentage of applications with documentation is file
Purpose	To make sure that IT systems police exist and well documented
Implementation Evidence	• How many organisations have IT policy • Is the national ICT policy in place?
Frequency	Annually
Formula	Number of organisations with policy to Total number of surveyed organisations
Data source	Documentation repository/ National public documents
Indicator	The target is to 100 percent. As the percentage approach 100 it is an indication good best practice

The Center for Internet Security *Concensus Metric Definitions* document also provides a great guide to define metrics and data attributes.

Identify the data owners that provide the Security Scorecard content. This is important for many organizations in which the Security team is not be centralized. Resources may be matrixed to perform security duties. For example, the firewalls are administered by the network team, virus prevention is administered by the PC team, and vulnerability management is administered by the security team. Collectively and collaboratively these teams make up the organization's "security team". This means the data owners for the Security Scorecard are across multiple teams and possibly departments. Using the RACI, document the data owners that provide the Security Scorecard metrics. Discuss the level of effort to produce the data on a recurring basis and identify any opportunities for time saving automation. Confirm service levels align with the frequency of update desired for the Security Scorecard.

Determine how the data should be segmented. For example, determine if the metrics should be divided up for specific communities (e.g., by geographic location, by business unit, by regulatory requirement, etc.). A composite view may be necessary when the nature of the vulnerability dictates the team that will be engaged for remediation efforts. For example, there may be value separating vulnerability data by product defect and configuration error. Product defects are followed by security updates, patches, or mods. These defects are a result of vendor quality control issues. Product defect requires the vendor to release a code update. Once a patch is released, the Release Management team deploys the software update. On the other hand, a vulnerability caused by a configuration error may require a revision to the system build standard and IT staff education. Segmentation is very important so that the audience quickly sees their reflection in the metrics and recognizes information that is pertinent.

7.4. Develop

Do not depend exclusively on technology and tools to obtain data and create a Security Scorecard. Avoid creating a data gathering effort that is overly complex or level of effort high. A balance is recommended. Attestation of control state and compliance may be appropriate to consider. When reporting on a metric, a level of uncertainty can be

stated. The Security Scorecard will be a living document, requiring routine updates (e.g., monthly or quarterly). Remember that complexity is the nemesis of repeatability.

During this phase, the initial layout of the Security Scorecard is created. When creating the artifacts within the Security Scorecard (e.g., pie charts, line graphs, etc.) consider the level of effort necessary to routinely update the data. Consider mimicking the look and feel of existing business scorecards that were shared during the executive interviews. This way the audience is familiar with format.

Distribution mechanisms should be developed to get the Security Scorecard into the target audience's hands. There are several options including email and web portals. Emailing the Security Scorecard as an attachment is typically adopted early. As time passes, the security professional may find this approach does not provide much feedback as to who is actually reading the Security Scorecard. Another approach is to use an internal web server or portal to post the content. A kindly reminder may be appropriate by sending an email to the target audience with an embedded URL that launches the browser to the location on the web server with the latest Security Scorecard. Authentication can be performed transparently (e.g., AD integrated IIS) so that reader's account name is recorded when the browser presents the credentials in the background. This will provide a convenient method for the audience to retrieve the Security Scorecard as well as a convenient method for the security professional to track who is actually interested and routinely reading the latest Security Scorecards. Feedback mechanisms should also be incorporated so that the Security Scorecard audience can ask questions or make suggestions for improvement. This is especially true for the pilot.

Creating a standard operating procedure (SOP) document is very valuable for service quality and consistency. Unfortunately, this common requirement for IT operations is not considered for publishing recurring scorecards or KPI reports. During the development phase, an SOP should be created that describes the routine activities necessary to maintain and update the Security Scorecard content. The SOP scope is not just for the security professional related activity. It should include the activities performed by all staff that provide the sources of data for the Security Scorecard. If for example the Security Scorecard contains virus prevention statistics, the resources and

duties that must be performed to create the data set should be documented in the SOP. Developing the SOP will help foster conversation with the staff managers regarding necessary service levels and continued availability of resources. Performing resource planning with staff managers and data owners will be greatly appreciated. This planning is valuable to avoid heroic efforts for every update.

7.5. Test and Revise

Testing begins with a small pilot group for feedback on the Security Scorecard content. To avoid premature action on the metrics presented, consider using artificial data first. This way the pilot group will not spring into action based interpretation of the data. The primary goal of the pilot is to ensure the Scorecard contains the data type necessary to support decision making. The actual data values of the metrics during this phase is not critical—ensuring the right data types for metrics have been identified is most important.

Exercise the distribution and feedback mechanisms described above. This provides two major benefits. The first benefit is the audience becomes familiar with how the Scorecards are to be delivered routinely in the future. The second benefit is the security professional has a way of tracking participation in the pilot.

Revise SOP documentation and try to quantify effort for recurring activities. Confirm with staff managers that actual time demands to perform update duties aligns with forecasted level of effort and duration. These findings will have a strong influence on the frequency of updates to the Security Scorecard.

Documenting and sharing lessons learned is very valuable. As the pilot team reviews and interprets the data, sharing their perspectives and recommendations will foster further improvement. Capturing this quality improvement information in some form of on-line knowledge base can be helpful to the security professional as well as the Security Scorecard audience.

This phase is intended to be iterative. Do not enter into this phase with the expectation that a "once and done" approach will be successful. Continuous evaluation of Security Scorecard content is important. Ideally members of the pilot team will be

able to see their "reflection" in the Security Scorecard. Remember, not all metrics are meaningful. Be sure to regularly confirm with the pilot team Security Scorecard content relevance.

7.6. Deploy

This phase begins with the final, approved Security Scorecard content and layout. Now the distribution begins. Consider calling a meeting or authoring a broadcast email targeting the Security Scorecard audience. Revisiting the presentation material shared during the project kick-off meeting will be appreciated as a significant amount of time may have passed. As the Security Scorecard product may be the result of a collaborative effort among multiple teams, this may be a good time for recognize this contribution. Offer breakout sessions with stakeholders to review the Security Scorecard content. This will help ensure that the relevant information is being identified, content is being interpreted correctly, and the call to action is understood. Lastly, set expectations on how frequently updates to the Security Scorecard will be released (e.g., every 1st of the month, one a quarter, etc.).

As mentioned earlier in the design phase, tracking the access to the Security Scorecard is important to understand more about the consumer behavior. A broadcast email with the Security Scorecard as an attachment does not provide a convenient feedback mechanism to track the Security Scorecard review. In addition, this creates a potential security risk as the attachment will have weak or no access controls. Consider an existing internal web portal, document management system, or file share that tracks access to the Security Scorecard by logon name. An email with an embedded URL\UNC can be a convenient communication alternative to the attachment approach. Reports can then be run that reveal top readers of the Security Scorecard and reveal the ideal candidates to approach for feedback. Soliciting feedback is one of the best ways to keep the content relevant and audience engaged.

As teams attempt to act on the information presented in the Security Scorecard, they may request additional supporting data (sometimes referred to as "drill down" or "supporting" data). Be prepared to share this information as this may be necessary for delegation of work. For example, the Security Scorecard may show that multiple web

applications share a common vulnerability. However all the web applications may not have been developed by the same team or may have been contracted to third-parties. Be prepared to provide access to the source data to help identify the right teams to assign remediation efforts. Monitor how this supporting data is used. Knowing how the data is used may provide insight into additional metrics that are relevant and valuable for the Security Scorecard.

7.7. Maintain

After the initial release of the Security Scorecard occurs, feedback may drive changes to scope and content. Drivers include changes in organization objectives, market behavior, risk conditions, and leadership motivation. This is normal and considered a natural progression. As with SDLC, this Security Scorecard approach is cyclical to drive continuous improvement. The scope and content do not have to remain static.

The Security Scorecard is a decision support tool. Once decisions are made and objectives achieved, new content may be necessary reflecting this organizational dynamic. The Security Scorecard content can then evolve to assign a small amount of "real estate" confirming controls are sustained in their desired state, and more space dedicated to emerging risks. This is acceptable and in many ways considered a successful organizational adoption of the Security Scorecard. Follow change management procedures and document these improvements to the Security Scorecard. Keep to the practice of limiting scope so that the Scorecard does not grow to an obligation that is not sustainable.

As time passes, a baseline will develop. Consider updating the Security Scorecard metrics to include this historical perspective in addition to point in time status. In some cases the trending or trajectory is as important as the current moment in time metric value. For example, security update implementation might be at 85%. This may seem undesirable at this time, however a trend may reveal an improvement of 10% month over month for the last 3 months. Extrapolating this data reveals that compliance should be achieved within 45 days. This risk timeline may be acceptable to the organization.

8. Conclusion

The Security Scorecard is an effective communication tool that can help organizations with risk management and strategic decision support. Benefits include:

- Improve security program
- Increase accountability
- Increase credibility
- Improve awareness
- Justify resource investment and prioritization
- Advance organizational efforts to reduce risk

Managing the Security Scorecard is a cyclical process—not a once and done effort. As with continuous improvement initiatives, the Security Scorecard contents will evolve to reveal organization capability maturity and provide focus on critical risks to the organization. The return on this investment is one of the best ways to provide executives relevant and actionable information about the state of security program for the organization.

9. References

Andrew Jaquith. *Security Metrics : replacing fear, uncertainty, and doubt*. Upper Saddle River, NJ : Addison-Wesley.

Andrew Jaquith (March 2010). Proving Your Worth. *Security Information Magazine* (p29).

Brotby, W. K. *Information Security Metrics : A definitive guide to effective security monitoring and measurement*. Boca Raton, FL : Auerbach Publications.

Center for Internet Security Consensus Metric Definitions v1.0.0 (2009). Retrieved August 1, 2010 from https://www.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.0.0.pdf.

Corporate Information Security Working Group Report of the Best Practices and Metrics Teams (2005). Retrieved August 1, 2010 from http://net.educause.edu/ir/library/pdf/CSD3661.pdf.

Michael Hoehl, mmhoehl@gmail.com

Debra S. Herrmann. *Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI* . New York, NY : Auerbach Publications.

Dean R. Spitzer. *Transforming Performance Measurement: Rethinking the Way We Measure and Drive Organizational Success*. New York, NY : Amacom.

Dennis Opacki. *Security Metrics : Building Business Unit Scorecards* (2005). Retrieved August 1, 2010 from http://www.adotout.com/BU_Scorecards.pdf.

Gene Kim, Paul Love, etal. *Visible Ops Security: Achieving Common Security and IT Operations Objectives in 4 Practical Steps.* Eugene, OR : IT Process Institute.

James Quinnild, Jeff Fusile, Cindy Smith (Feb, 2006). Why information security belongs on the CFO's agenda. *Healthcare Financial Management*. Retrieved August 1, 2010 from http://findarticles.com/p/articles/mi_m3257/is_2_60/ai_n16069809/?tag=content;col1

Jessica Keyes. *Implementing the IT Balanced Scorecard: Aligning IT with Corporate Strategy*. New York, NY : Auerbach Publications.

Job Asheri Chaula, Louise Yngström, and Stewart Kowalski, Department of Computer and Systems Sciences, Stockholm University/KTH (2008). *Security Metrics and Evaluation of Information Systems Security* . Retrieved August 1, 2010 from http://icsa.cs.up.ac.za/issa/2004/Proceedings/Research/048.pdf.

Kahraman, E. (2005). *Evaluating IT security performance with quantifiable metrics*. Retrieved September 1, 2010 from http://www.dsv.su.se/en/seclab/pages/pdf-files/2005-x-245.pdf.

Lance Hayden. *IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data.* New York, NY. : McGraw-Hill.

National Institute of Standards and Technology (NIST) Special Publishing 800-55 *Performance Measurement Guide for Information Security.*

National Institute of Standards and Technology (NIST) Special Publishing 800-33 *Risk Management Guide for information Technology Systems.*

National Institute of Standards and Technology (NIST) Interagency Report 7564 *Directions in Security Metrics Research.*

National Institute of Standards and Technology (NIST) Interagency Report 7358 *Program Review for Information Security Management Assistance (PRISMA).*

Ronda Henning, etal. *Proceedings of the Workshop on Information Security System Scoring and Ranking*, Applied Computer Security Associates, Williamsburg, Virginia, May 21-23, 2001. Retrieved August 1, 2010 from http://www.acsac.org/measurement/proceedings/wisssr1-proceedings.pdf.

SANS SEC504 Hacker Techniques, Exploits and Incident Handling Course Content (2010).

SANS MGT512 SANS Security Leadership Essentials For Managers with Knowledge Compression™ Course Content (2007).

Tom Patterson. *Mapping Security*. Upper Saddle River, NJ : Addison-Wesley.

Scott Berinato. *A Few Good Information Security Metrics*, CSO Magazine, July 01, 2005. Retrieve July 1, 2010 from http://www.csoonline.com/article/220462/A_Few_Good_Information_Security_Metrics?contentId=220462&slug=&.

SSE-CMM: Systems Security Engineering Capability Maturity Model, International Systems Security Engineering Association (ISSEA). Retrieved July 15, 2010 from http://www.sse-cmm.org/metric/metric.asp.

U.S. PCI DSS Compliance Status. (2010). Retrieved August 1, 2010, from http://usa.visa.com/merchants/risk_management/cisp_merchants.html.

Wim Van Grembergen and Steven De Haes. *Enterprise Governance of Information Technology: Achieving Strategic Alignment and Value.* New York, NY : Springer.

Appendix A: Security Scorecard Project Checklist

- ✓ Create statement of objectives
- ✓ Establish target audience and stakeholders
- ✓ Create a formal project charter and plan
- ✓ Present plan and obtain letter of authorization from CIO to stakeholders
- ✓ Host project kick-off meeting (ideally with CIO present)
- ✓ Identify major organizational and business unit objectives
- ✓ Review recent audit reports and recommendations
- ✓ Author questions for Executive Interview(s)
- ✓ Perform executive interviews to identify key risk concerns and priorities
- ✓ Establish inventory of security controls associated with mitigation of aforementioned key risks
- ✓ Identify roles for security controls using RACI and identify associated sponsors ($)
- ✓ Research benchmarks and authoritative sources for security controls (e.g., best practices, quality standards, etc.)
- ✓ Research relevant regulation and contract obligations
- ✓ Identify and document metrics that are to be presented in Security Scorecard
- ✓ Establish data sources and data owners
- ✓ Creation/Selection of tools to gather data and create Security Scorecard
- ✓ Draft Security Scorecard template
- ✓ Circulate template and request comment based on RACI$
- ✓ Perform resource planning with functional managers and data owners
- ✓ Establish communication protocol for Security Scorecard audience
- ✓ Pilot first draft of Security Scorecard
- ✓ Document Security Scorecard update procedures
- ✓ Document lessons learned and make appropriate corrections to Security Scorecard
- ✓ Finalize Security Scorecard layout and content
- ✓ Establish Feedback mechanisms
- ✓ Formally announce Security Scorecard
- ✓ Close project

Appendix B: Security Scorecard RACI

This appendix provides an example RACI document based on Payment Card Industry (PCI) Data Security Standard. The RACI is versatile and can be used to map roles and responsibilities for any security program.

PCI Data Security Standard 1.2 Requirements

Requirements	Priority	Larry Lead	Steve Smart	Michale Manager	Adam Act	Greg Guru	Harry Helpful	Network	Systems	Security	CIS	IT Standards of Excellence: ITIL	ISO	COBIT
Requirement 1: Install and maintain a firewall configuration		MANAGERS			STAFF			OFFICERS						
1.1 Establish firewall and router configuration standards that include the following:	6	A	I		R			I		I	x	x	x	x
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	6	A	I		R			I		I	x	x	x	x
1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks	1	A	I		R			I		I	x	x	x	x
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	2	A	I		R			I		I	x	x	x	x
1.1.4 Description of groups, roles, and responsibilities for logical management of network components	6	A	I		R			I		I	x	x	x	x
1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure	2	A	I	I	R	C		I		I	x	x	x	x
1.1.6 Requirement to review firewall and router rule sets at least every six months	6	A	I		R	C	R	I		I	x	x	x	x
1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.	2	A	I		R	C	R	I		I	x		x	
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.	2	A	I		R		R	I		I	x		x	
1.2.2 Secure and synchronize router configuration files.	2	A	I		R		R	I		I	x	x	x	x
1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	2	A	I		R		R	I		I	x		x	
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	2	A	I		R		R	I		I	x		x	

The RACI document is a matrix used to clarifying roles and responsibilities for cross-functional/departmental security duties. It is a very valuable tool to document this understanding as well as identify gaps in duty assignments. Project Managers use this tool frequently when leading a multi-team initiative.

There are a few variations of RACI, but all have in common (R)esponsible, (A)ccountable, (C)onsult, and (I)nform. Definitions are provided below:

Responsible – Individual(s) performing the work

Michael Hoehl, mmhoehl@gmail.com

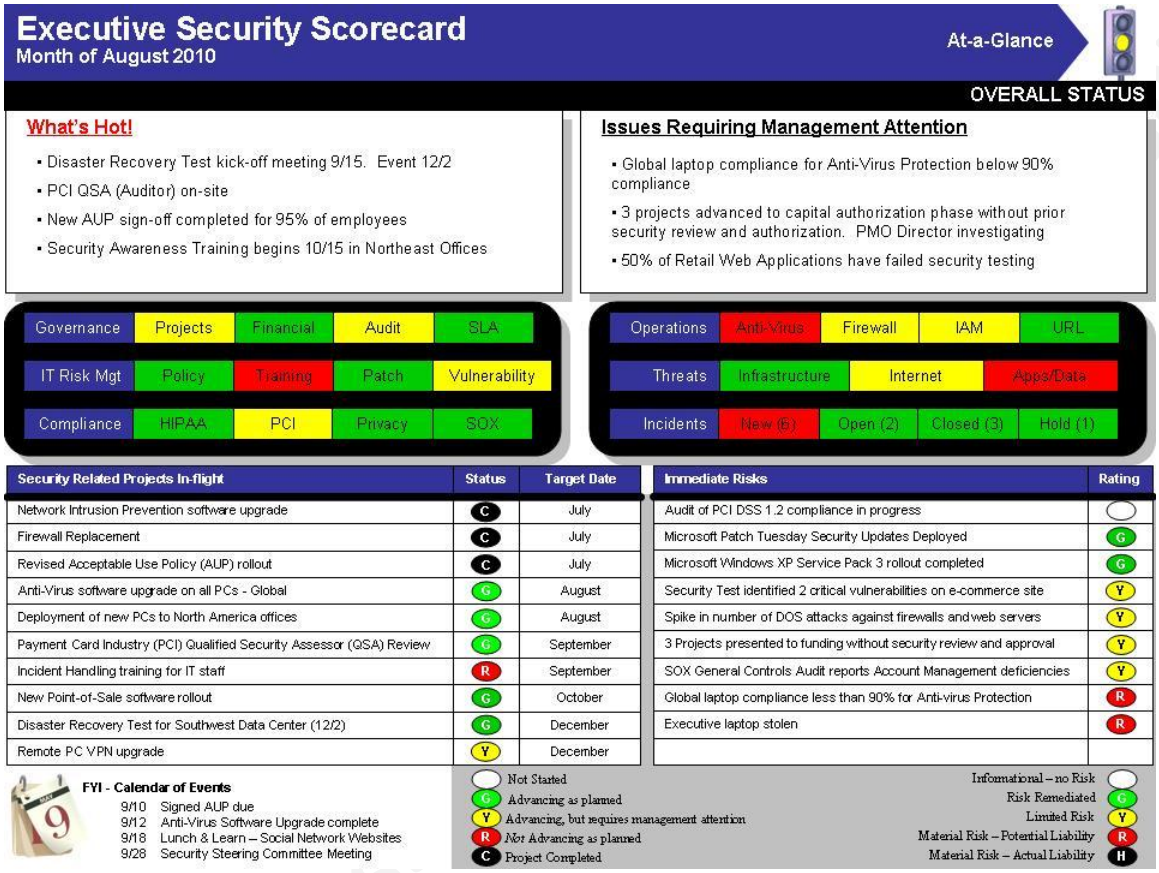
Accountable - Individual who are obligated and ultimately manage correct and thorough completion. The one to who manages Responsible and ensure work is done and compliance is sustained. Common practice is to ensure only one Accountable individual is specified for each duty or deliverable.

Consult – Individual(s) providing expert or management guidance, but not specific duties or recurring tasks.

Inform – Individual(s) kept up-to-date on progress and compliance. Often this is a stakeholder or sponsor. Typically this is a one-way communication.

Appendix C: Security Scorecard Example

Below are examples of summary and drilldown Security Scorecards for reference.



Executive Security Scorecard
Month of August 2010

At-a-Glance

OVERALL STATUS

What's Hot!

- Disaster Recovery Test kick-off meeting 9/15. Event 12/2
- PCI QSA (Auditor) on-site
- New AUP sign-off completed for 95% of employees
- Security Awareness Training begins 10/15 in Northeast Offices

Issues Requiring Management Attention

- Global laptop compliance for Anti-Virus Protection below 90% compliance
- 3 projects advanced to capital authorization phase without prior security review and authorization. PMO Director investigating
- 50% of Retail Web Applications have failed security testing

Governance	Projects	Financial	Audit	SLA
IT Risk Mgt	Policy	Training	Patch	Vulnerability
Compliance	HIPAA	PCI	Privacy	SOX

Operations	Anti-Virus	Firewall	IAM	URL
Threats	Infrastructure	Internet	Apps/Data	
Incidents	New (6)	Open (2)	Closed (3)	Hold (1)

Security Related Projects In-flight	Status	Target Date
Network Intrusion Prevention software upgrade	C	July
Firewall Replacement	C	July
Revised Acceptable Use Policy (AUP) rollout	C	July
Anti-Virus software upgrade on all PCs - Global	G	August
Deployment of new PCs to North America offices	G	August
Payment Card Industry (PCI) Qualified Security Assessor (QSA) Review	G	September
Incident Handling training for IT staff	R	September
New Point-of-Sale software rollout	G	October
Disaster Recovery Test for Southwest Data Center (12/2)	G	December
Remote PC VPN upgrade	Y	December

Immediate Risks	Rating
Audit of PCI DSS 1.2 compliance in progress	
Microsoft Patch Tuesday Security Updates Deployed	G
Microsoft Windows XP Service Pack 3 rollout completed	G
Security Test identified 2 critical vulnerabilities on e-commerce site	Y
Spike in number of DOS attacks against firewalls and web servers	Y
3 Projects presented to funding without security review and approval	Y
SOX General Controls Audit reports Account Management deficiencies	Y
Global laptop compliance less than 90% for Anti-virus Protection	R
Executive laptop stolen	R

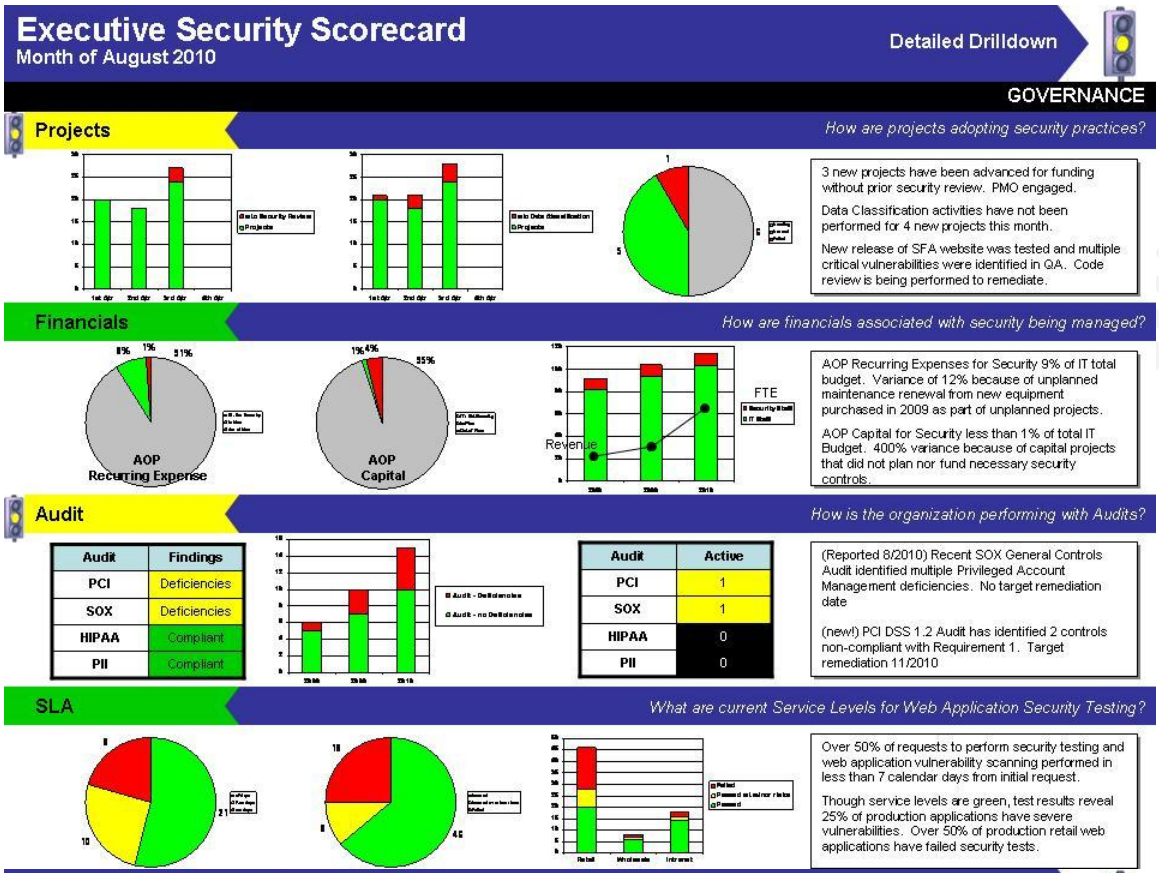
FYI - Calendar of Events

9/10 Signed AUP due
9/12 Anti-Virus Software Upgrade complete
9/18 Lunch & Learn – Social Network Websites
9/28 Security Steering Committee Meeting

Not Started
G Advancing as planned
Y Advancing, but requires management attention
R *Not* Advancing as planned
C Project Completed

Informational – no Risk
Risk Remediated G
Limited Risk Y
Material Risk – Potential Liability R
Material Risk – Actual Liability H

Michael Hoehl, mmhoehl@gmail.com



Michael Hoehl, mmhoehl@gmail.com