Security Metrics

Building Business Unit Scorecards

December 2005

Dennis Opacki, CISSP
dopacki@covestic.com

Abstract: The ability to measure the specific contribution of business unit behavior to overall organizational risk is increasingly important to today's security leaders. This paper explores two methods of producing business unit security metric scorecards, examining metric selection, data acquisition, and challenges inherent to each approach.

Table of Contents

1.0 Overview

Security managers are increasingly turning to security metric scorecards, hoping to produce buttoned-up business cases for spending, and drive accountability outwards to business units. Though recent articles on security metrics have approached scorecards as data visualization exercises[1], one problem remains; measuring an immature organization's performance is difficult. Producing effective security metric scorecards takes great diligence in metrics definition, data gathering, reporting and communication.

2.0 Benefits

Despite challenges inherent in developing scorecards, there is great business value. Security metric scorecards are important tools for:

- Finding hot spots of risk within the organization
- Precisely targeting remediation
- Measuring internal compliance with organizational policy
- Discovering broken internal processes
- Taking advantage of security-related sunk costs

When developing security scorecards, it is important to understand there are two types of metrics. First, there are those metrics which measure how effective central security efforts are in driving down risk. These metrics capture the delta between current risk and some needed end-state, presumably a lower net risk. They help answer the question, "is our organization doing what it should be doing?" As a significant body of literature discusses developing this class of security scorecard, this paper will explore an alternate view, the *business unit security scorecard*.

Business unit security scorecards present metrics, which measure the risk inherent in the delta between end user behavior and organizational policy. These metrics are important in that they drive accountability for risk. Metrics in this class answer the question, "are we doing what we say we are doing?". They should also map directly to organizational policy.

3.0 Methodology

There are two distinct approaches to developing security scorecards, top-down and bottom-up. While both approaches provide similar decision-support data for business managers, companies should select an approach based on current organizational maturity, project scope and available funding. The top-down approach is more formal and comprehensive, allowing stakeholders to define needs and objectives. Nimbler and less

[1] Berinato, Scott. *A Few Metrics*. In CSO Online. http://www.csoonline.com/read/070105/metrics.html

formal, the bottom-up approach enables organizations with immature security programs to speed scorecard development.

3.1 Top-Down Approach

With a top-down approach to scorecard development, business leaders and subject matter experts partner to define key security indicators for the organization before collecting data.

3.1.1 Stakeholders

Involving the correct stakeholders is instrumental to creating a security metric scorecard, which accurately represents business objectives. Stakeholders and their responsibilities include:

- Information security leadership – Define overall security metrics program objectives and measurement areas
- Security subject matter experts – Translate objectives and measurement areas into security metrics and data needs
- Security control owners – Confirm measurement objectives and data needs against existing control evidence, and install instrumentation

3.1.2 Metric Definition

Metrics suitable for business unit scorecards meet the following:

- They contain information necessary to support business unit correlation
- Business unit behavior directly influences them; they are not indirect measurements of central information technology or security efforts
- All business units contribute data to them
- They measure behavior the business unit is accountable for

Good metrics tie closely to business objectives, program maturity, and the company's control environment. Some possible areas of measurement may include:

- Security and privacy awareness participation
- Requested or approved high-risk policy exceptions
- Worm or virus infections among business unit staff
- Central management systems, such as SMS or antivirus found disabled
- Time to install software patches (if the business units apply their own patches)
- Lost or stolen mobile computers
- Rogue wireless access points discovered
- Delay between employee termination and manager seeking access shutoff

- Spyware and adware infections
- Software license violations
- Improper content possession (e.g. MP3s or pornography on file shares)
- Unsecured or unmanaged source code or sensitive data archives
- Business unit vendors undergoing security approval
- Business unit policies, procedures and controls undergoing risk analysis

Pay careful attention to the story metrics tell about business unit behavior. Adjust metrics as necessary for business unit size, if it creates a more compelling story. The National Institute of Standards (NIST) offers a special publication, which may be useful in selecting security metrics[2]. Remember, defensible metrics are the key to an effective scorecard.

3.1.3 Instrumentation and Data Collection

When installing control instrumentation to promote collection of metric data, look first to existing sources of information, such as application log files and manual audit trails. For controls with no record-keeping, install instrumentation at choke-points, such as entry, internal handoffs, and completion. It is important to ensure there are no flow paths around the instrumentation.

Once instrumentation is in place, allow enough time to ensure reasonable data collection, before performing validity checking. A pilot period, perhaps close to thirty days should ensure data collection across all business units. A short pilot period may increase the difficulty of discovering whether acceptable statistical distribution is present. Business units may use certain processes or systems occasionally; the longer the pilot period, the easier it becomes to confirm data.

Few business leaders have the necessary risk appetite to sponsor lengthy pilot periods. Given common misconceptions about the relative ease of reporting security metrics, the longer an effort goes without producing metrics, the less likely it is to garner continued business management support.

3.1.4 Challenges

There are several reasons it may become necessary to revisit the instrumentation and collection tactics for specific data:

- Data doesn't correlate to specific business units
- Poor statistical distribution of data across business units is present
- *Leaky processes* allow multiple paths to the same result
- Controls change during the measurement period

[2] Swanson, Marianne., Bartol, Nadya., Sabato, John., Hash, Joan., Graffo, Laurie. *Security Metrics Guide for Information Technology Systems.* (2003). National Institute of Standards Special Publication 800-55.

3.2 Bottom-Up Approach

To meet expectations, some organizations select a bottom-up approach to metrics development. Here, organizations perform a technical assessment of available security-related data, and select performance indicators. While the bottom-up approach yields quicker results, the first generation product will not contain all relevant security performance indicators.

3.2.1 Data Acquisition

Finding data to support business unit security scorecards can seem a daunting task. It is important to start small. Work with information security leadership to gain an understanding of overall information security program objectives. Reflect these objectives in the metric strategy; if compliance is a key program objective, consider examining controls that help enforce compliance.

Schedule meetings with control owners and carefully explain the objectives of the scorecard effort. Data owners may be reluctant to share their data for several reasons, including:

- Territoriality – in some organizations, data equates to power[3]; asking for data may imply a request to give up control
- Perceived sensitivity – well-intentioned employees may have an inflated opinion their data's sensitivity, or poor knowledge of proper data classification
- Insecurity –employees may feel concerned that data they share will reflect poorly on their performance

Relieve these concerns by describing how the control owner stands to benefit from participation in the business unit scorecard program. The scorecard will highlight their controls and contribution, and increase the effectiveness of their controls by holding end users accountable for risky behavior.

Carefully review data produced by security controls for metric relevance. Raw data, which support measurement of business unit behavior, should meet the following criteria:

- They contain the necessary information to support correlation to a specific business unit
- Business unit behavior influences them; they are not indirect measurements of central information technology or security efforts
- All business units contribute to the data
- They measure behavior the business units are accountable for

[3] Demarest, Marc. (1997). *The Politics of Data Warehousing.* http://www.noumenal.com/marc/dwpoly.html

Consider data collected automatically, and discuss with data owners, ways to further automate data collection. Look for opportunities to gather added data, given minor control changes.

3.2.2 Data Assessment

A common challenge faced in assessing data's metric relevance is that control operators often collect only tactical data. This is common with technical controls, such as firewalls, intrusion detection systems, and system process monitors; these controls produce so much data that without pruning or summarization, storage becomes problematic. Unfortunately, if data owners prune, summarize or discard the fields which make their data suitable for metric generation, we risk being unable to report behavior related to these controls on the business unit scorecard.

In the worst case, scorecard data collection may run afoul of corporate policy. Data suitable for the scorecard may have special handling needs because of business sensitivity or privacy protection; control owners may be unable to extend their data collection to include suitable data without added funding for security countermeasures. Next, data destruction policies may increase the difficulty of preserving enough raw data to support scorecard creation; at a minimum, these policies increase the difficulty of performing trend analysis. Last, scorecard data may be discoverable, in a legal sense; companies should consider legal aspects of collecting business unit scorecard data.

Carefully examine data to discover candidate metrics, considering the manner in which they directly and indirectly show business unit contribution to risk.

Examples of direct indicators include:

- Employee malware incidents (worms, viruses, spyware)
- Employee custodianship of sensitive data (PDAs, laptops, file shares, access credentials)
- Circumvention of controls, such as unauthorized access

Examples of indirect indicators include:

- Approved behavior, in exception of organizational policy
- Employee awareness of security policy
- Employee participation in manual processes (patching, antivirus updates, data destruction)

After selecting key indicators and the most suitable data fields to represent them, consider adjusting metrics for business unit size, number of computers, or other high-

level indicators. The most compelling and defensible metrics have good denominators, meaning the larger the sample size, the more reliable they are likely to be. Support selected metrics by correlating supporting data to business units. Reexamine metrics supported by data with poor statistical distribution across business units; it is critical to select metrics which reflect behavior consistent across all business units.

Select a single target for each metric, balancing between achieving risk-reduction goals and ensuring business unit acceptance of the scorecard. Base your targets on overall organizational security objectives, current performance of business units, and political considerations such as business unit amenability to outside scrutiny. Bear in mind that early scorecards dripping with red ink are unlikely to garner long-term business unit support.

Decide the relative importance and weight of each metric in the greater context of the scorecard. Having the flexibility to assign higher or lower weights to individual metrics will go a long way towards engaging business units in scorecard refinement. If business units voice valid reasons they believe particular metric have unduly influenced their overall score, produce an updated scorecard with new weights. A key part of scorecard success is business unit acceptance (discussed in more detail in the *Communication* section below); your goal is to keep the focus on the targets and weights, not the data or method.

3.3 Correlation

As the primary purpose of a business unit security metrics program is to assess business unit behavior contributing to overall risk, you must attribute raw data to business units. Perform this in two steps. First, attribute raw data to individuals. Next, attribute individuals to organizations.

3.3.1 Technical Attribution

There are a few ways to attribute data to individuals; however, each presents a unique challenge. Perhaps the most straightforward way of correlating data is by e-mail alias, assuming this is a valid organizational database field. If not, it may be necessary to produce and manually keep a translation table between alias and another key field, such as employee identification number or full name.

Other data provide similar, though perhaps more formidable challenges:

Internet address

Many companies use Dynamic Host Control Protocol (DHCP) to assign Internet addresses (IP). To correlate an IP address to an individual, it may be necessary to cross-reference data time stamps with the recorded IP address with DHCP logs. You may need to develop custom tools, as DHCP servers often store their logs directly on the server, and often in a format which does not lend itself to ready correlation.

Network address translation (NAT) allows many computers to use a single IP address, making it challenging to attribute noted behavior to specific individuals. Network administrators often configure NAT devices to discard the translation information necessary to correlate individuals to IP addresses.

Location

Employees connected to a corporate network by Virtual Private Network (VPN) connections may appear as if physically present in the office. Also, many teams often share VPN facilities, making it challenging to attribute VPN use to specific individuals. Use VPN access logs to correlate IP addresses found in logs to credentials. Then, cross-reference credentials with access control systems to identify users.

Wireless users are often difficult to identify, as wireless access points deal out a shared pool of addresses. In fact, many wireless access points act as DHCP servers, and keep no records of address assignment. In this case, correlate common application server logs to map wireless addresses to users.

Machine Name

Most computers in today's office environment have many users. Assuming you can programmatically list a machine's accounts, try to find criteria that help you attribute computer use to a specific user. While a simplifying assumption may be to assign data related to this computer to all users with accounts, this may result in counting data multiple times, if many users are part of the same business unit. A better approach may be to consider the most recently logged-in user, or the user with the most login time as the owner. Still, this approach has a key weakness in that computer users are not necessarily computer owners.

3.3.2 Organizational Hierarchy

Once you identify key data fields to support business unit correlation, select an authoritative hierarchy. Organizations often have multiple hierarchies serving different business needs. The most familiar of these hierarchies is the *reports-to* hierarchy. This basic tree defines employee reporting, and represents the view of the company one would expect to see on an organizational chart.

While it may seem natural for the scorecard to reflect this, it is not without challenges. First, the database representing the reports-to hierarchy may be more difficult to traverse in one direction than the other. For example, discovering an employee's manager may be easier that listing a supervisor's direct reports. Poor company data architecture can increase the complexity of scorecard data correlation. Second, company databases may not capture less-formal, but equally important *dotted-line* reporting, and reporting information for contractors and consultants.

Another possible hierarchy is the *cost center* view commonly used by finance departments to track revenue and expense attribution. This hierarchy is likely more

complete and accurate than the reports-to hierarchy. However, an organization's financial hierarchy may be unfamiliar to many managers, resulting in confusion over accountability for cost center performance. To confuse matters further, in larger organizations, the cost center hierarchy may be comptroller-centric, rather than mapped to management. As the senior finance representative within a business unit is rarely accountable for information security, it will still be necessary to identify the senior manager within each business unit.

While you can perform business unit correlation manually, it is cumbersome and inefficient. Business unit scorecard construction will likely require custom stored procedures and queries, to support correlation. Also, as you are collecting and correlating data from multiple sources, a dedicated database may be necessary. Finally, scorecard data may represent significant business or privacy risk; set up necessary controls to protect your data.

3.3.3 Drill Down

An important decision in producing a business unit security scorecard is how deep to allow scorecard recipients to drill down. As the high-level view offered by the scorecard is its primary value, it does not necessarily make sense to allow users to view all underlying data. First, deep drill-down will highlight the sparse nature or absence of data at the deepest levels. As decision support only needs high-level metrics, sparse data does not quash the scorecard approach. However, wide visibility into data distribution draws scorecard discussion away from results and improvement, and towards method.

Deep drill-down may also limit the effectiveness of the business unit scorecard as a management tool. Deming believed that it is counterproductive to measure employee contribution individually[4]; employees who believe a security metrics program focuses on singling out poor performers are unlikely to support the effort. As we will explore later, successful security metrics programs need wide organizational acceptance.

Finally, deep drill-down increases the difficulty of producing a security metric scorecard. In a midmarket to large organization, document or spreadsheet-based scorecards may reach their scaling limits at three to four levels of visibility. Beyond this level, scorecards either become resource-intensive software development projects, or rigid and difficult to update monsters.

3.3.4 Challenges

A security metric scorecard must be flexible enough to support the myriad organization realignments common in today's organization. As organizational changes alter scorecard roll-up and the resulting metrics, it is often difficult to analyze trends. The decision-support value of security metrics relies on the ability to isolate impact of decisions on business unit metrics over periods of time, a problem made more difficult when the organization changes during a measurement window.

[4] *Deming: Teachings*. (2000). The W. Edwards Deming Institute website. http://www.deming.org/theman/teachings02.html

Scorecard automation plays a significant role in deciding the difficulty of responding to organizational changes. Spreadsheet-based scorecards may need significant effort to keep, while data warehouse-centric solutions often respond transparently. An organization's restructuring frequency should be a consideration in deciding whether to employ a manual spreadsheet or document-based scorecard, or an automated scorecard tool.

3.4 Communication

3.4.1 Scorecard Views

There are differing schools of thought on whether to allow business units to see company-wide results, or just those about their business unit. One theory is that allowing all units access to the executive view will drive competition and collaboration between business units. Security metrics pundit Andrew Jaquith[5] states,

> "the act of publishing each [business unit's] scores starts spurring conversation between the [business units]. Poor performers call the best performers to ask for tips and share information. The rising tide lifts all boats, as it were."

Another possibility is, given access to company-wide results, egregiously poor performers will withdraw support for scorecard efforts or undermine data collection. The results will depend on the organization's political culture.

At a minimum, it will be helpful to produce an *executive view* of the scorecard. The executive scorecard should contain some or all the following:

- A high-level view of the business units, showing their scores alongside other business units
- A calculated score or index for each business unit, considering individual metric weights
- A calculated score for the entire company, possibly an average or weighted average of business unit indexes
- Metric descriptions, including their significance, data source, and formulas and tables used to weight and score data
- Metric-specific guidance, describing what behavior drives the metric, and how business units can improve their scores
- Copies of the individual business unit scorecards showing fill drill-down

[5] Jaquith, Andrew. (2005). Personal Interview. *http://www.securitymetrics.org*

If you consider it undesirable to give out the executive scorecard to individual business units, produce a business unit-centric view. It should contain the following:

- A high-level view showing business unit scores versus targets and company-wide averages

- Metric descriptions, including their significance, data sources, formulas and tables used to weight and score data

- Business unit-specific guidance, describing behavior driving metrics, specific areas for improvement, and how the business unit can improve their scores in these areas

- A copy of the individual business unit scorecard showing full drill-down

3.4.2 Communication Models

How you communicate the scorecard to individual business units can be as important as the findings it contains. Just because the scorecard has executive sponsorship does not necessarily imply it will be successful. Avoid an excessively prescriptive first release, enabling better collaboration with business unit stakeholders. With such collaboration, an organization is more likely to negotiate a livable solution for all business units, which improves security without alienating key players.

There are several potential scorecard communication techniques, including *catcher/pitcher* and *poster child*. In the catcher/pitcher model, each business unit appoints a liaison to coordinate with the central security team. The business unit liaison acts as a remediation project manager, working with members of the central security team. Together, they define the best path to metric improvement. The progress achieved through this consultative model may be slow, and may require significant hand-holding from the central security team.

In the poster child model, business units take full ownership of compliance, based on prescriptive guidance provided by central security. Hard-charging early adopters are the first to realize increased metric scores, giving them an opportunity to tout their efforts with executive management. Other business units may quicken or retarget improvement efforts once they understand what is effective. This approach works best when you convince the lowest scoring business unit to become the poster child.

3.4.3 Challenges

If you do not carefully communicate the business unit scorecard, or if business units feel you are measuring them unfairly, they may try to discredit the scorecard. There are several ways a business unit can attack the underlying data or scorecard method:

- Incomplete data – Business units may point out leaky processes, where there are multiple ways to getting the same result. Unless your instrumentation and data

gathering capture all paths to the objective, business units may claim your picture of them is incomplete.

- Meaningless metrics – Business units may claim that chosen metrics do not adequately link to business unit behavior or organizational policy. Scorecard owners must clearly define the link between metrics, policy and business unit behavior.

- Exceptional circumstances – Business units may claim that their circumstances or business priorities require behavior inconsistent with organizational policy. Remind business units that it is the scorecard's role to capture and report risk, and that although approved, their behavior still adds to net organizational risk. Further, representing this risk on the scorecard may help them gain funding and support for compensating controls or safe, long-term solutions.

- Ignorance of standards – Business units may plead ignorance of the standards you measure them against. Even if correct, the scorecard properly reflects organizational risk resulting from business unit behavior. Now that they are aware of proper behavior, there is significant opportunity to improve their metric results.

- Correlation confidence – Business units may question the confidence with which data correlates to them, possibly citing the challenges described in *section 3.3.1*.

- Weighting and scoring – Business units may challenge the weights assigned to individual metrics, or metric targets. While these are negotiable to a certain extent, it is important to be clear about why you select certain targets and weights.

- Selective Improvement – Business units may work to improve metrics rather than the underlying security control they are intended to measure, for the sole purpose of improving scorecard results.

Bear in mind that a business unit's political goal is not necessarily to derail the security metrics program, but to avoid accountability for the measured period. Anticipate and develop responses to challenges; do not defer measurement in hopes of discovering ideal data or methods. Remind business units the business unit security metrics are merely indicators of business unit behavior. However, don't be shy about supporting your assertions with underlying data.

4.0 Summary

Developing a security metric scorecard is a worthwhile effort, which will provide useful insight into the overall risk posture of a company's business units, as well as the behavior driving unnecessary risk into the business. Managers can use security metrics to better target funds for security remediation, drive accountability for risk outwards to business unit management, or as a first step in dividing information assurance capacities across corporate business units.