Ramon Krikken

Analyst

Security and Risk Management Strategies

Burton Group

Field Research: Security Metrics Programs

Security Metrics Programs

Field Research: process, timeline, and demographics

- Focus on security governance and management topics
- In-depth interviews with senior-level security management
- Spanning 30 organizations; 25 in North America, 5 in Europe
- Private sector only; no government or educational institutions
- Interviews conducted between February and April 2009

Financial Services	7	Insurance	2
Computer HW/SW	4	Pharmaceuticals	2
Health Care	3	Transportation	2
Retail	3	Travel	1
Manufacturing	3	Media	1
Energy	2		

Security Metrics Programs

Summary of findings

- Frameworks for metrics programs vary greatly
- Metrics programs are at varying levels of maturity
- A wide range of measurements is collected
- A limited range of metrics is reported to management
- Perceived success often related to business / culture
- Metrics programs are increasingly formalized

Security Metrics Programs

Most participants act on perceived utility

Risk metrics measured at various levels, during projects and for existing processes and infrastructure

Incident metrics measuring rates of occurrence, impact to the organization, and resolution efforts

Operational metrics measuring a variety of processes and technologies on status, effectiveness, and efficiency

Compliance metrics relating to performance in the previous categories

Visible trend towards formal metrics programs and review boards, but maturity and the perceived success of the program wildly vary

Security Metrics Programs

Some participants speak about perceived futility

"No one has ever been able to measure security—executives only care about the incidents that impact the business."

"Success is really binary—it was prevented or not. If there's no impact, then no one cares that it was prevented."

"Quantitative measurements of security can't be done."

Exhibited in two ways: what metrics are collected by whom, and how they are (**or are not**) communicated to executive management

Framework for Metrics Program

- Organizations vary in metrics program focus
  - Some security groups focus on results/outputs
  - Some groups focus on controls and compliance
  - Technical metrics relate to exceptions and are generated by tools
  - SLAs are used to set targets that are subsequently tracked
  - Economic model *may* be used to assess effectiveness of controls
- Value of metrics can be hard to show in business context
  - "If the business continues to run then that's success"
  - Cannot always easily connect security success and failures with impact on the business goals (particularly in certain verticals)
  - Showing ROI, other than cost savings, is still hard for many

Security Metrics Programs

Low-level security metrics and measurements

- Low level metrics are produced by security tools, such as SIEM, vulnerability management, DLP, etc:
  - Number of laptops protected with full drive encryption
  - Number of fully patched systems
  - How quickly patches are deployed
  - How long it takes to remediate a vulnerability
  - Number of vulnerabilities per line of application code
  - Audit finding mitigation in place
  - Results of vulnerability scans
  - Number of malware/virus incidents
  - Percentage of systems with latest AV signatures
  - Number of trouble tickets concerning security
  - Number of DLP policy violations

Risk metrics

- Risk metrics tend to be subjective and hard to quantify
  - Lack of formal risk metrics and process in some organizations
  - Likelihood information is often inaccurate
  - Relative risk is easier to work with than absolute risk
  - Map to industry best practices whenever possible
  - Metric thresholds and dashboards help to focus (red, yellow, green)
- Results of assessments and audits are important metrics
  - Several organizations measure themselves by improvement
  - Benchmarking is mentioned, but only by few organizations
- Exceptions to policies and standards are tracked
- As expected, interpretation of risk is highly contextual

Incident metrics

- Many organizations (as expected) track incidents
- Data breach metrics sometimes assigned a dollar cost
  - No strong indications of benchmarking
- However, not all organizations view things the same way
  - Definitions of what is an incident vary at the detail level
  - Some definitions are "text-book," others more contextualized
- Business context again determines what matters
  - Several interviewees commented that management does not necessarily care about all incidents; only about business impact

Security Metrics Programs

Metrics and measurements reported to management

- Number of security assessments performed
- Exceptions to compliance policies
- Application risk scores
- Internal and external audit findings
- Security awareness attestations, surveys, and test results
- Incidents and related costs
- Satisfaction surveys
- Compliance with internal and external service level agreements (SLAs) such as for security operations requests
- Security group budget and accuracy of project cost estimates
- Status of active security projects
- Payment Card Industry Data Security Standard (PCI DSS) compliance status and dates met

Security Metrics Programs

Metrics reporting and use

- Tactical operational security metrics are reported on weekly/monthly basis
  - Operational or technical security metrics are used within IT security organization and IT Operations, but are not useful to senior execs
- Several cases where CISO explicitly notes management is not interested in operational metrics or even security incident metrics
- Security status and security project status are often visible to senior management and board oversight groups
  - Focus on how well policy and controls are implemented
  - Results of awareness testing, assessments, and audit findings
  - Identify compliance exceptions or important *operational* incidents

Security Metrics Programs

Relationship to Compensation

- Metrics that can show performance improvement are more visible and may impact compensation/bonus
  - Personal and team objectives per role, but *not* tied to incident metrics
- Security organization objectives for improvement and team bonus may be tied to metrics/dashboard
  - Several cases where this is tied to security operations efficiency
  - Other cases where it is tied to security budget management
- In some cases CISO compensation is based both on hard numbers and assessment by peers
  - In one case a survey was used to assess alignment with the business
  - One CISO noted this relates to “how others [business] feel about security”

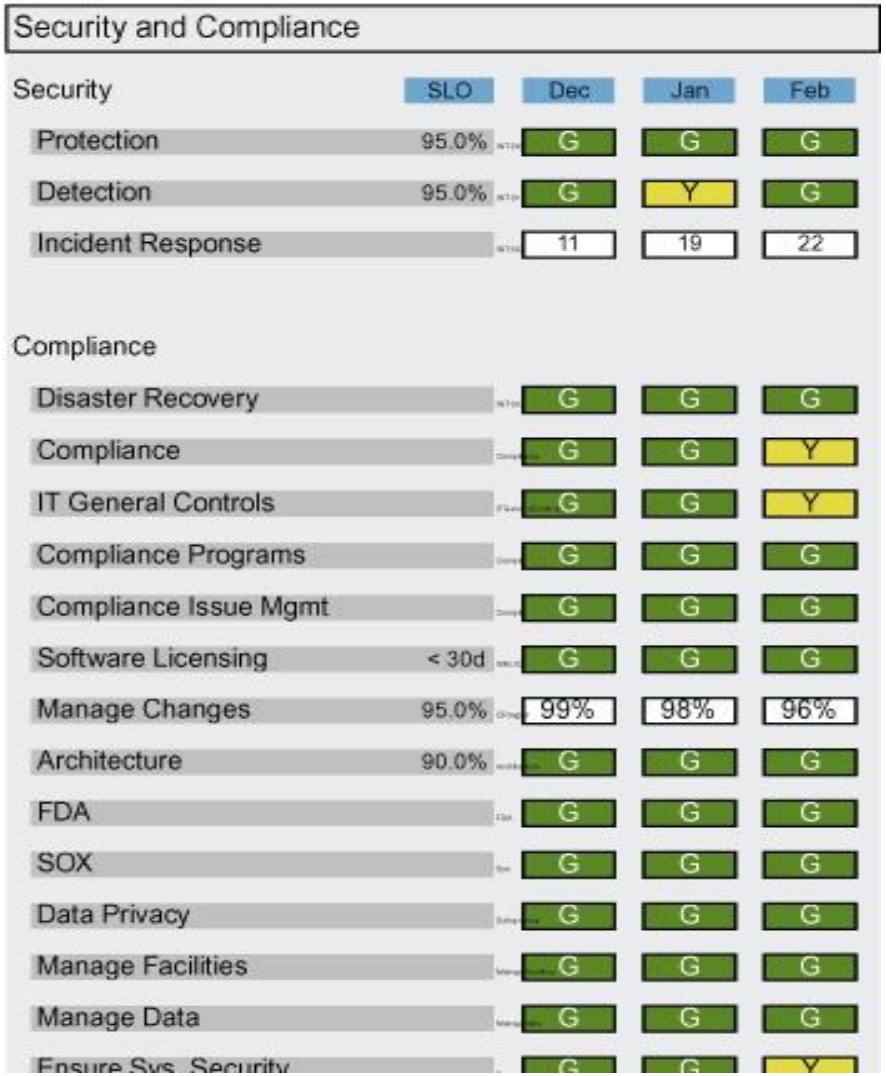
Security Metrics Programs

Reporting, tools, and dashboards

- Organizations are moving towards greater automation in their metrics programs
  - Some examples where Archer's suite is used to aggregate metrics data from other sources
  - Some use of dashboards that are based on internal spreadsheets
    - Manually compiled from variety of sources, including security tools
    - Spreadsheets are still at the top of data management for metrics!
  - Scorecards that assess BUs or sites against a set of controls
  - Track exceptions to policy and progress towards remediation
  - One CISO notes to "only gather the data you plan to use"
    - Indication of information overload?

Security Metrics Programs

Example of Operational Security and Compliance Dashboard



Conclusions

- Some organizations appear successful in creating and communicating metrics that connect with business goals
- A fair number of interviewees experience disconnects with management, and some doubt metrics are doable
- There is still a large gap between low-level operational metrics and mid-level program and management metrics
- Effective positioning/operation of the security team(s) appears vital to develop effective metrics programs

Security Metrics Programs

Related Burton Group Research and Recommended Reading

- "Security Key Performance Indicators "
- "Security Metrics: Horses for Courses"
- "Introduction to Key Risk Indicators"
- "Thinking Strategically About Security Metrics"
- "Using Metrics Effectively: Proving and Improving the Business Value of IT"
- "You Manage What You Measure"