Metrics That Matter – Security Risk Analytics

Katy Loughney, Director of Risk Analytics, West - Brinqa
May 15th, 2014
What Matters to CIOs?

**Priorities**
From a technology perspective, which of the following is your highest priority?:

- Business Intelligence / Analytics
- Infrastructure and Data Center | 10%
- Cloud | 10%
- Mobile | 8%
- Enterprise Resource Planning | 8%
- Cybersecurity

http://online.wsj.com/news/articles/SB10001424052702304680904579364641778947268?mod=ITP_journalreport_0
IT Professionals Do Not Communicate Security Risk

September, 2013 - Tripwire, Inc., released results from an extensive study focused on the state of risk-based security management with the Ponemon Institute. Key findings from the survey include:

- 64% said they don’t communicate security risk with senior executives or only communicate when a serious security risk is revealed
- 47% said that collaboration between security risk management and business is poor, nonexistent, or adversarial
- 51% rated their communication of relevant security risks to executives as “not effective.”
- When asked why communicating relevant security risks to executives was not effective:
  - 68% of the respondents said communications are too siloed
  - 61% said communication occurs at too low a level
  - 61% aid the information is too technical to be understood by non-technical management
  - 59% said negative facts are filtered before being disclosed to senior executives and the CEO

http://www.prweb.com/releases/2013/9/prweb11095496.htm
Analytics is the process of Signal Detection

“You gotta help me stop looking up stuff I don’t actually care about.”
The Signal and The Noise

Data are neither signal nor noise - data are merely facts. When facts are useful they serve as signals. When they aren’t useful, data clutter the environment with distracting noise.

For data to be useful, they must:

- Address something that matters
- Promote understanding
- Provide an opportunity for action to achieve or maintain a desired state

Without these qualities, data is noise.
Why Do We Need Security Risk Analytics?

A common request from the leadership is to report on metrics from various areas that point out which businesses, processes, or systems are most at risk and require immediate attention.

- Risk reporting based on business context
- Compliance is no longer the driver
- Risk prioritization rather than risk elimination
- Big data and automation
Operational Metrics are NOT Risk Metrics

Operational metrics to benefit operational efficiency

- Percentage of YTD spending of security budget
- Percentage of completion of annual objectives
- Percentage of confidence of completing objectives
- Number of new processes created and implemented
- Project status (major, per project)
- Percentage completed
- Percentage of confidence of completion
- Number of compliance deficiencies, last audit
- Number of remaining open compliance deficiencies

Source: Gartner, Inc.
Key Challenges
Key Challenges In Implementing Risk Analytics

- Varied and disparate risk inventories
  - Uncorrelated and redundant data included in reporting
  - Prohibits establishing a common inherent risk inventory
  - No historical data for trending and forecasting

- Manual and inconsistent data aggregation and correlation
  - Ambiguous and incomplete risk interpretation
  - Resource and time intensive

- Subjective and non-standard risk measurement
  - Resources spent addressing non-prioritized issues
  - Miscommunication and misunderstanding of risk across enterprise

- Operational teams lack understanding of business outcomes
  - Limits business unit’s ability to understand and accept risk
  - Inability to measure improvements and predict threats
  - Reactive vs. proactive decision making
Gartner Redefining GRC Space in 2014

- Vendors use it to describe whatever they are selling and clients use it to describe whatever problem they have

- 2014 approach to GRC will deemphasize the presence and demonstrability of features and functions while increasing the weight of implementation and production use of GRC products against specific use cases
  - Use case 1: IT Risk Management (ITRM)
  - Use case 2: Operational risk management (ORM)
  - Use case 3: Audit management
  - Use case 4: Vendor risk management (VRM)
  - Use case 5: Business continuity management (BCM)
  - Use case 6: Corporate Compliance and Oversight
Technology Risk Analytics Use Case
1. Collection of data from multiple inventory sources
2. Integration of enterprise-wide control data and manual controls (i.e., SOC, IT SOX control)
3. Automated risk ranking process
4. Formulate report data into the integrated risk assessment warehouse (central version of the truth)
5. Automatic processing of assessment, analytics, and calculation metrics (prioritize risk, predictive analysis, business intelligence)
6. Produce output to information consumers (e.g., Risk Officers see patch levels for apps/business)

High Inherent Risk + High Risk Control = High Residual Risk (to be escalated)
- GRC
- SIROs
- IT Reports
- Information Risk Management
- Other reports
Context Based Security Risk Metrics
Basic Active Directory User Admin Metrics

- **9.66%** - Active Idle Perpetual Accounts
- **61.35%** - Active Perpetual Accounts
- **98 : 1066** - Ratio of Failed Login Attempts (vs) Total Active User Accounts

**Mean Password Age**
- Chart showing distribution of password ages.

**Accounts by Account Expiration Type**
- Bar chart showing accounts by expiration type.

**Mean Password Expiration**
- Bar chart showing mean password expiration times.
Trending Metrics

Application Risk Trend

Issues By Domain and Gap
Infrastructure Metrics

Non-certified Accounts on Critical Database: 2
Critical Vulnerabilities older than 90 days: 295
Most Impacted Server: nyginwebp4.us.xyz.com
Sensitive Database with Critical Vulnerabilities: 18.18%

Systems with Known Missing Patches

System Issues by Datacenter

brinqa | Smart Metrics, Intelligent Decisions
Risk Analytics Case Studies
Law Firm – Compliance Risk

- 3 offices
- Fewer than 500 Employees

- Partners at firm decided to put enhanced emphasis on security & risk policies, controls, and assessments
- Only security/risk information available was from an application pen test (last conducted by outside firm in 2012)
- Starting with the basic blocking and tackling but looking to enhance capabilities over time

- Intelligent Risk Assessments
  - More robust than a spreadsheet
  - Ability to track changes / progress over time
  - Workflow analysis
Healthcare Organization – Compliance Risk

- Regional healthcare operation
- 20 locations include hospitals, research facilities, nursing homes, administration

- Have been involved with HIPAA / HITECH risk assessments
  - Highly manual process
  - Time consuming to coordinate spreadsheets and word documents within SharePoint

- Intelligent Risk Assessments
  - Customizable views for executive, analyst, and compliance teams
  - Ability to launch new assessments and incorporate dynamic changes based on new regulatory requirements
Higher Education – Compliance Risk

- Two billion dollar educational institution with 9 campuses, 17,000 faculty and staff, and undergraduate and graduate students exceeding 110,000

- Numerous, complex challenges to manage and maintain compliance and risk reporting among the 9 different campuses and multiple departments within each campus

- Needed to consolidate multiple risk management initiatives to meet their specific compliance needs and to maintain consistency and visibility across the entire institution

- Automated assessment engine – consistent assessments led to greater efficiencies and more manageable risk

- Created centralized risk repository for campus-wide risk reporting

- Flexible reporting
Fortune 100 Financial Institution – Vendor Risk

- Managed 1500 vendors with risk posture only reported at vendor level
- Vendor programs in use were fragmented and manual
- Vendor adherence and accountability to corporate policy was difficult to enforce

- Centralized repository to capture vendor profile, services provided by vendors, assessments, and evidences
- Integration with D&B, Lexis Nexis, and change detection system (Google Alerts) to capture and notify on breaches in real time
- Risk engine to provide quantitative risk scoring and statistical risk modeling to present the vendor risk posture in a normalized scheme

- Increased efficiency and transparency in vendor risk program
- Centrally hosted solution reduces the overall operating costs and provides easy mechanism of data exchange
Financial Clearing Corporation – SDLC Risk

- Lacked common taxonomy for representing risk related to app sec issues
- Lacked common repository to provide holistic view of security information
- Lacked standard framework for representing risk and exposure
- Could not identify most critical issues impacting their application portfolio

- Automated SDLC process with criteria defined by quantitative modeling to determine application lifecycle state
- Ability to measure trends of app risk scores with data warehouse
- Customized visibility for business owners and management

- Prioritization of issues based on risk to organization
- Clear and consistent information on risk posture
- Ability to predict and respond to threats
World’s Largest Deposit Bank – TRM Risk

- Unable to provide businesses with repeatable risk metrics
- Unable to provide actionable remediation plans with accountable parties
- 21 different assessments resulted in overlapping and N/A control testing
- Assessments did not look at all available data

- Streamlined all 21 assessments to avoid overlapping & out of scope questions
- Leverage IT monitoring tools to validate risk assessment answers and enable real-time visibility of controls
- Use a centralized technology risk assessment repository to reduce complexity, improve operational efficiency, and focus remediation expenditures

- Standardized, streamlined, and centralized TRM process for consistency
- Incorporated data from existing IT controls (DLP, patch mgmt, etc.)
- Achieved sustainable constant monitoring of current technology risk for the enterprise, not just one time assessments
- Provided granular self-service views of technology risk for a department, business unit, and entire enterprise
- Historical and predictive technology risk simulations using customer’s data in context
About Brinqa

Brinqa provides a risk analytics platform for aggregation, correlation, analysis and reporting of risk data in heterogeneous environments. The solution delivers insightful analysis and intelligent reporting for informed decisions and improved operational effectiveness.
Contact Information:

Katy Loughney – Director of Risk Analytics, West
kloughney@brinqa.com