Metrics that Matter – Security Risk Analytics

Rich Skinner, CISSP
Director Security Risk Analytics & Big Data
Brinqa
rskinner@brinqa.com

April 1\textsuperscript{st}, 2014.
“You gotta help me stop looking up stuff I don’t actually care about.”
Agenda

- Challenges in Enterprise Security, Risk
- Analytics & Industry Views
- Introduction to Security Risk Analytics
- Building Business Context into Risk / Security Programs
- Example Case Studies
- Q&A
2014 Security, Risk Landscape
Compliance Is No Longer the Driver. Risk.

Source: Gartner
### Global CIO Top 10 Technologies

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Analytics and business intelligence</td>
<td>1</td>
<td>1</td>
<td>5</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>Mobile technologies</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>6</td>
<td>12</td>
</tr>
<tr>
<td>Cloud computing (SaaS, IaaS, PaaS)</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>16</td>
</tr>
<tr>
<td>Collaboration technologies (workflow)</td>
<td>4</td>
<td>4</td>
<td>8</td>
<td>11</td>
<td>5</td>
</tr>
<tr>
<td>Legacy modernization</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>15</td>
<td>4</td>
</tr>
<tr>
<td>IT management</td>
<td>6</td>
<td>7</td>
<td>4</td>
<td>10</td>
<td>*</td>
</tr>
<tr>
<td>CRM</td>
<td>7</td>
<td>8</td>
<td>18</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>Virtualization</td>
<td>8</td>
<td>5</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Security</td>
<td>9</td>
<td>10</td>
<td>12</td>
<td>9</td>
<td>8</td>
</tr>
<tr>
<td>ERP applications</td>
<td>10</td>
<td>9</td>
<td>13</td>
<td>14</td>
<td>2</td>
</tr>
</tbody>
</table>

* Not an option in that year
5 Macro Trends in Security / Risk

Security & Risk Professionals Should Focus on 5 Macro Trends

1. The data economy will ensure the dominance of data-centric security
2. **Analytics will help you better predict threats and protect your data**
3. Human elements will drive security re-orgs, training and outsourcing
4. S&R leaders will play a bigger role in customer experience
5. Business resilience is taking on broader corporate implications – security risk, IT failures, data corruption, etc.

Source: 2013 Top Trends to Watch, *Forrester, Inc.*
How to improve Intelligence = Analytics

What is “Analytics”?

Analytics is the discovery and communication of meaningful patterns in data. Especially valuable in areas rich with recorded information, analytics relies on the simultaneous application of statistic, computer programming and operations research to quantify performance.

http://en.wikipedia.org/wiki/Analytics
What is ‘Big Data’?

- Webopedia -- Big Data Definition

- Big data is a **buzzword**, or catch-phrase, used to describe a massive volume of both **structured** and unstructured **data** that is so large that it's difficult to process using traditional **database** and **software** techniques. In most enterprise scenarios the data is too big or it moves too fast or it exceeds current processing capacity.
What is 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.

- Business context based risk reporting
- Compliance is no longer the driver
- Risk prioritization not risk elimination
- Big data and automation
Current State of Risk ‘Intelligence’

<table>
<thead>
<tr>
<th>Cause</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual and Inconsistent data collection</td>
<td>Ambiguous and unreliable interpretation of risk</td>
</tr>
<tr>
<td>No central risk repository or historical data</td>
<td>Uncorrelated and redundant data included in risk analysis</td>
</tr>
<tr>
<td>Subjective risk measurement and prioritization</td>
<td>Valuable time and resources wasted addressing non-critical risks</td>
</tr>
<tr>
<td>Lack of business context and no holistic view of risk</td>
<td>Inability to measure improvements and predict threats</td>
</tr>
</tbody>
</table>
Info Security HAS a Risk Analytics Problem

- Application Vulnerabilities
- Compliance Monitoring
- Privacy Monitoring
- Business Relevant Data
- User Activity Monitoring
- Identity And Access Data
- External Threat Intelligence Data
- Network Data
- Network Vulnerability Information
- Privileged Activity Monitoring
- Performance Monitoring
- Transaction Monitoring
- Sensor Data
- Log Data
- Configuration Information
- Context Aware Data
- Change Management Information
- Volume
- Variety
- Velocity
- Complexity

Smart Metrics, Intelligent Decisions
Current State Of Technology Risk

Risk and Compliance

Security Operations

SIEM
DLP
IAM
Firewall
IDS/IPS Configurations
Endpoint Protection
Antivirus
Patch Mgmt
Vulnerability Mgmt
Gartner = Re-defining GRC Space, again

- GRC = Governance, Risk, & Compliance
- Gartner one of the leading world-wide analysts firms has had multiple definitions of GRC throughout the years

- Here is 2014 version:
  - Examine Use Cases instead of generic categories

- 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.
Building Business Context into Risk / Security Programs
What Metrics are important to YOUR organization?

- How many vulnerabilities reported year by year?
- External Threat Intelligence?
  - Real-time attacks
  - Industry wide zero day exploits
- Mean time to mitigate fixes? Too generic?
- % of Critical Systems with known issues?
- Critical Security Issues by each Line of Business?
- Which of my Business assets are at CyberSecurity Risk?
- What security / risk controls are failing across my enterprise by business unit?
- What countries pose the biggest threats to current worldwide enterprise?
Financial Services Example - Challenges

Financial Services Company has a model where an application supports multiple process and business unit. The risk assessment process needs to keep this context in mind while compiling the risk assessment score.

- The hierarchy presented was the following
  - Business Unit
    - Process support BU
      - Application tied to process

- A single application may be tied to multiple process and multiple business unit

- The inherent risk computed for the application has to take this process and business unit in consideration while evaluation the inherent risk of an application

- In addition, the control assessment is conducted only once against the application
To elaborate further, the risk model takes into account the different context (risk profile – application) for the same application to compute inherent risk. However, the control assessment is done **ONCE** and the corresponding residual risk for the application risk profile is updated.
Methodology

Step 1: Consolidate Data

Step 2: Contextualize Info

Step 3: Automate Issue Life Cycle

Step 4: Prioritize Issues

Step 5: Support Business Decisions

- Map Information
- Business
- IT
- GRC

Common Taxonomy & Automated Workflow

Smart Metrics to prioritize issues

Reports, Dashboards

Smart Metrics, Intelligent Decisions
Ultimate Risk Analytics End Goal

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 sees patch levels for apps/business)
Case Studies

- Entry Level
  - Small Organization: Law Firm
- Intermediate
  - Small Organization: Healthcare
  - Medium Organization: Higher Education
  - Large Organization: Global Technology
- Advanced
  - Large Organization: Financial Institution
Regional Law Firm

- 3 Regional Offices
- Less than 500 Employees Total
- Partners at firm decided to put enhanced emphasis on Security & Risk Policies, Controls, and Assessments
  - Starting with the basics but looking to enhance capabilities over time
- Application Security, Penetration Testing was last conducted by outside firm in 2012
- Conducting Enterprise Risk Assessment for first time
  - More than just a excel spreadsheet
  - Ability to track changes / progress over time
  - Workflow analysis
Healthcare Organization

- Regional Healthcare Operation
- 20 Locations Across One Particular State
- Hospitals, Research Facilities, Nursing Homes, Administration

Due to HIPAA / HITECH have been involved with Risk Assessments for the last couple of years
  - Very Manual Process
  - Long hours involved within process and coordination of multiple spreadsheets, word documents within Sharepoint.

Intelligent Risk Assessments
  - Executive Views / Analyst Views / Compliance Views
  - Ability to launch new assessments and incorporate dynamic changes
Higher Education

- 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 viability across the entire institution.

- Enterprise Risk Management (ERM)
- Compliance Obligation
- Third Party Vendor Risk
- HIPAA Compliance
- Device Retirement
Global Technology Firm

Customer Profile
- Fortune 50 global technology company
- Over a million reported vulnerabilities from various systems
- Lack of visibility and identification of key risk areas

Security Risk Analytics Solution
- 2-3 Hour processing of vulnerabilities within the system
- Consolidation and remediation by Application instead of individual vulnerabilities
- Quantitative risk analysis
- Central warehouse for all issues, risks and findings
- Closed loop remediation for host vulnerabilities
Financial Institution

Customer Profile
- Fortune 100 global financial institution
- 2400 critical applications
- Lack of visibility and identification of key risk areas
- Costly labor to address thousands of issues/findings yearly

Security Risk Analytics Solution
- Portal to report infrastructure components and applications
- Integrated asset model to show the relationship between applications and supporting infrastructure
- 800 Critical Applications, 17000 servers, 1000 databases
- Simulation analysis to produce reports based on scenarios
Financial Institution

- Large Financial Clearing Corporation that connects thousands of financial institutions worldwide
- Lacking visibility into worldwide application security
- Groups were focused on individual areas
- Lacking Enterprise View

Solution
Integrating Application Security Analytics within the SDLC Process

- Technology
  - Penetration Testing
  - Source Code Review / Analysis
  - Version / Regression Testing

- Users
  - Application Developers
  - Risk Managers
  - Security Managers
Metrics that Matter
Basic Metrics with User Admin (Active Directory)
Basic Metrics with User Admin (Active Directory)

9.66%  Active idle Perpetual Accounts

61.35%  Active Perpetual Accounts

9:1066  Ratio of Failed Login Attempts (vs) Total Active User Accounts

Mean Password Age

Accounts by Account Expiration Type

Mean Password Expiration
Trend Analysis
Country Risk Metrics

5.4 Times Risky

WTA Admin
Function-Highest Risk

-7.9 %
Offshore-Risk Change

Philippines
Country-Highest Risk

2.5 %
Onshore-Risk Change

Function by Country
Application Risk Metrics

Smart Metrics, Intelligent Decisions

Topics

Control Deviations / Gaps
Audit Metrics
Metrics That Matter

2
Non-certified Accounts on Critical Database

295
Critical Vulnerabilities older than 90 days

nyginwebp4.us.xyz.com
Most Impacted Server

18.18%
Sensitive Database with Critical Vulnerabilities

Systems with Missing patches

System By Criticality

Critical
High
Medium
Low

Patches Missing

Overall Overall

System Issues by Datacenter

New York

Count

Log Management
Patch Management
Vulnerability Management
Incident and Problem Management

Critical
High
Medium
Low

About Brinqa

Brinqa provides an operational 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.
Risk Analytics Platform

Brinqa risk analytics provides organizations **visibility** into all **essential data** and the **metrics** needed to **proactively** offset potential threats.

- **Data Aggregation and Correlation**
  - Advanced Correlation
  - Dynamic Surveys
  - Smart Connectors
  - Big Data Architecture

- **Context Aware Risk Models**
  - Best practice based
  - Risk Taxonomies
  - Easily configurable
  - Simulation models
  - Quantitative and Qualitative calculations
  - Adjustable threshold and tolerance levels

- **Dynamic Dashboards and Reports**
  - Risk prioritization, what-if analysis and trends
  - User-defined dashboards and reports
  - Role-based views
Contact Information:

Rich Skinner, CISSP
Director, Security Risk Analytics & Big Data
rskinner@brinqa.com
260.312.1958