DIGITAL RISK MANAGEMENT

Andy Waterhouse
EMEA Presales Director

Twitter: @Andy_J_W
WITH DIGITAL TRANSFORMATION, DIGITAL RISK IS THE GREATEST FACET OF RISK THAT BUSINESSES FACE.
By 2020, 60% of digital businesses will suffer major service failures, due to the inability of IT security teams to manage digital risk.

– Gartner
GRC
IT
SECURITY
GRC
CEO / BOARD
DIGITAL RISK
VISIBILITY
INSIGHTS
ACTION
IT
V
I
A

RSA
CRITICAL DOMAINS

For Managing Complex Challenges
**SECURITY OPERATIONS REQUIREMENTS**

**VISIBILITY**

- Users, devices, endpoints, infrastructure, and applications
- Data from all pieces of their infrastructure including physical offices, virtual data centers and public clouds
- Make sense of large data sets – Metadata

**INSIGHTS**

- Overlay Threat Intelligence onto the data they collect
- Variety of Detection Rules and *User and Entity Behavioral Analytics*
- Connect various pieces of seemingly disparate events to gain insight into targeted campaign

**ACTION**

- Quickly investigate incidents with detail all the way down to the user and machine to understand root cause
- Orchestrate and automate repetitive investigations
VISIBILITY
- Engage cross functionally to set a wide aperture of risk
- Feed with the business' objectives, assets, resources and third party relationships
- Integrate a diverse and broad set of data sources

INSIGHTS
- Weigh identified risks against business context
- Leverage past incidents to help predict/prevent future incidents
- Develop a unified analysis of risk across risk domains

ACTION
- Track the steps, workflow, accountability and status of risk response actions
- Provide risk information back to the first line of defense to enable better business decisions
- Incorporate root cause analysis to continuously improve the process and risk outcomes
Visibility

- Quickly investigate incidents with detail all the way down to the user and machine to understand root cause
- Orchestrate and automate repetitive investigations

Insights

- Understand typical and anomalous usage patterns
- Identify new “good” patterns to establish new baselines

Action

- Challenge a user’s identity or transaction based on new context and insights
- Capabilities to terminate or limit a user’s access
CROSS DOMAIN REQUIREMENTS

SECURITY OPERATIONS

RISK MANAGEMENT

USER ACCESS
A unified, phased approach to provide visibility, insights, and action to manage digital risk

NEW REQUIREMENTS
CROSS DOMAIN EXAMPLE: Pulling Business Impact Analysis in Security Operations

- Security Operations teams (responsible for Exclusion) are short staffed and overwhelmed by alerts
- Pulling BIA from Risk Management into the SIEM can inform prioritization of both Visibility (what do I need to monitor) and Action (how do I respond to threats)
Example: UEBA applied to IAM

- IAM provides visibility of access request
- UEBA flags as abnormal and triggers action (step up auth) within IAM system

**Normal Access Request**

**Abnormal Usage; Step-up Authentication**
CROSS DOMAIN EXAMPLE: Aligning Consumer Fraud with Incident Management

- User Access feeds adaptive authentication case management data into Risk Management
- Risk Management builds Incident Management workflow and feeds into User Access platform

Adaptive Auth data / rules

Incident Management Workflow
LOS ANGELES WORLD AIRPORTS
Customer – Owner and Manager of LAX and Van Nuys Airports

“We need to make sure that our security posture consistently mirrors the needs of the organization… RSA understands the importance of this connection and provides us with the solutions that ensure that our security strategy is always driven by our business objectives.”
- Anson Fong, CISO

Issue
- Disparate threat intelligence, IT, Risk data

Solution
- RSA NetWitness Suite
- RSA Archer Suite
- Bring immediate context to security events from a single dashboard

Outcome
Improved quality and speed for incident response and recovery
"My goal is to leverage automation as much as possible, while at the same time, to push both visibility and accountability throughout the organization."

"RSA is one of the key partners I use to ensure that my organization accurately supports the company’s business goals."

- Vishal Salvi, CISO and SVP
**DIGITAL RISK MATURITY**

- **Siloed**
  - Ad Hoc, Reactive
  - Trigger Events
  - Tactical POV

- **Managed**
  - Platform Approach
  - Pervasive Visibility
  - Leverage Technology
  - Integrate Silos

- **Optimized**
  - Sharing and Collaborating Across Silos
  - Integrated business & risk context
  - Priorities and resources aligned with risk and business objectives
## Maturity in Four Key Areas

### RSA Risk and Cybersecurity Practice

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>Cyber Incident Risk Mgt</th>
<th>3rd Party Governance</th>
<th>Data Privacy Risk</th>
<th>Digital Business Resiliency</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ability to identify sophisticated attacks &amp; breaches, lateral movement, initial impact and effectively respond with a cross functional response</strong></td>
<td>Risk is considered from perspective of loss events, opportunity costs and enhancing likelihood of achieving objectives and executing strategy. Risk taking decisions are proactive</td>
<td>Business context is completely infused into compliance processes and technology. Monitoring capabilities alert stakeholders to impactful regulatory changes</td>
<td>Integrated information governance into corporate infrastructure and business processes to such an extent that compliance with program requirements and legal, regulatory, and other responsibilities are routine</td>
<td></td>
</tr>
<tr>
<td><strong>Ability to identify commodity malware, some breaches, some lateral movement, basic initial impact and respond with a somewhat coordinated cross functional response</strong></td>
<td>Management has information needed to understand complete context of risk. More informed decisions made and accountability established but decision process is still manual</td>
<td>System of record in place to manage full lifecycle of compliance activities. Stakeholders collaboratively define processes and policies; remediation activities are consistently monitored and reported</td>
<td>Established proactive information governance program with continuous improvement. Information governance issues and considerations routinely integrated into business decisions</td>
<td></td>
</tr>
<tr>
<td><strong>Limited ability to identify commodity malware, some breaches, some lateral movement, basic initial impact and limited ability to respond</strong></td>
<td>Agreement on risk management terminology, rating scales and assessment approach is established. Little business context is available and responsibility for each risk and control is not always clear</td>
<td>Operational standards and a comprehensive compliance catalog are developed. Some activity focused on improving effectiveness and stabilize processes with limited scope</td>
<td>Developing recognition that information governance has impact on organization and benefits from more defined program. Still vulnerable to scrutiny of legal or business requirements</td>
<td></td>
</tr>
<tr>
<td><strong>No ability to detect threats against the organization and no ability to respond when attacked</strong></td>
<td>Baseline activities are in place to manage risk but are isolated and fragmented. Beginning to obtain visibility into assessed level of inherent and residual risk but accountability is ad hoc</td>
<td>Organization understands broad compliance obligations but each area manages separately. Control performance is assessed ad hoc or as part of external audit</td>
<td>Information governance and recordkeeping concerns are not addressed at all, minimally or ad hoc. Will not meet legal or regulatory scrutiny or effectively serve the business</td>
<td></td>
</tr>
</tbody>
</table>

* Sourced from ARMA International Generally Accepted Recordkeeping Principles
# RSA RISK FRAMEWORKS

**Cyber-Breach Risk Framework: ABC Financial Services Company**

<table>
<thead>
<tr>
<th>Compliance Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>19 US State PII Laws, GDPR, PCI, &amp; FINRA Member</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Lowest Common Denominator Capabilities (partial list)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Plan, updated annually</td>
</tr>
<tr>
<td>Annual Audit Plan (PCI, Risk)</td>
</tr>
<tr>
<td>Maintaining event logs for 7 years</td>
</tr>
<tr>
<td>Real-time security event monitoring</td>
</tr>
<tr>
<td>Vulnerability scanning</td>
</tr>
<tr>
<td>72 Breach Notification</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Maturity Qualification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall Score: 50.4 out of 100</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Focus Breakdown:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-Breach Planning 5.7 out of 20</td>
</tr>
<tr>
<td>Operational Security 11.4 out of 20</td>
</tr>
<tr>
<td>Dwell Time Reaction 8.5 out of 20</td>
</tr>
<tr>
<td>Remediation 19.1 out of 20</td>
</tr>
<tr>
<td>Post-incident Handling 5.7 out of 20</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Overall Breach Readiness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average 10.8 per category, 3 points below average</td>
</tr>
</tbody>
</table>

---

**Prepare**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit and optimize operational IT and security</td>
<td></td>
</tr>
<tr>
<td>Cyber</td>
<td></td>
</tr>
</tbody>
</table>

**Detect**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber</td>
<td></td>
</tr>
</tbody>
</table>

**Analyze**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber</td>
<td></td>
</tr>
</tbody>
</table>

**Contain**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber</td>
<td></td>
</tr>
</tbody>
</table>

**Graduate**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber</td>
<td></td>
</tr>
</tbody>
</table>

**Recover**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber</td>
<td></td>
</tr>
</tbody>
</table>

**Post-Incident Handling**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber</td>
<td></td>
</tr>
</tbody>
</table>

---

**Pre-Breach (Pre-Breach) Preparedness**

<table>
<thead>
<tr>
<th>Left of Breach (Pre-Breach) Preparedness</th>
<th>Breach Risk Reduction (Breach Deflection)</th>
<th>Breach and Initial Incident Response</th>
<th>Breach Remediation</th>
<th>Right of Breach (Post Breach Adaptation)</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Cybersecurity Awareness and poor preparation is required</td>
<td>No Cybersecurity Awareness and poor preparation is required</td>
<td>No Cybersecurity Awareness and poor preparation is required</td>
<td>No Cybersecurity Awareness and poor preparation is required</td>
<td>No Cybersecurity Awareness and poor preparation is required</td>
</tr>
<tr>
<td>Cybersecurity Awareness and poor preparation is required</td>
<td>Cybersecurity Awareness and poor preparation is required</td>
<td>Cybersecurity Awareness and poor preparation is required</td>
<td>Cybersecurity Awareness and poor preparation is required</td>
<td>Cybersecurity Awareness and poor preparation is required</td>
</tr>
<tr>
<td>Cybersecurity Awareness and poor preparation is required</td>
<td>Cybersecurity Awareness and poor preparation is required</td>
<td>Cybersecurity Awareness and poor preparation is required</td>
<td>Cybersecurity Awareness and poor preparation is required</td>
<td>Cybersecurity Awareness and poor preparation is required</td>
</tr>
</tbody>
</table>

---

**Impact Analysis**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber</td>
<td></td>
</tr>
</tbody>
</table>

---

**Overall Breach Readiness**

Average 10.8 per category, 3 points below average
RSA PORTFOLIO

NETWITNESS’ PLATFORM
- Visibility across logs, network/packets, endpoint
- Behavioral analytics for accurate detection
- Orchestration and automation to speed response

SECURID’ SUITE
- Modern Multifactor Authentication
- Identity Governance & Lifecycle Management
- Identity Risk Management
- Convenient, Secure Access & SSO

FRAUD & RISK INTELLIGENCE SUITE
- Monitoring across Digital Consumer Lifecycle
- Risk-based Adaptive Authentication
- Integrated global Threat Intelligence
- Balance security and consumer experience

ARCHER’ SUITE
- IT Security Risk Management
- Cyber Risk Quantification
- 3rd Party Risk Management
- Compliance Management
- Operational Risk Management

RISK & CYBERSECURITY PRACTICE
- Digital Risk Maturity Assessment & Strategy
- Incident Response & Cyber-Defense Services
- Comprehensive Design and Implementation
- RSA University
- Customer Success
- RSA Communities

EVOLVED SIEM AND ADVANCED THREAT DEFENSE
- Secure Access Transformed
- Omni-Channel Fraud Prevention
- Proven Integrated Risk Management
- Advanced Risk and Cyber-Defense Services

BUSINESS-DRIVEN SECURITY™
RSA PARTNERSHIPS

400+ COMPANIES, 1000+ SOLUTIONS
RSA KEY STATS

30,000+ Customers

1 billion Consumers

50+ million Identities

400+ Global Technology Partners

94%
UNIFIED
Business Risk Management

ADAPTABLE
Advanced Security Operations

RESILIENT
Secure Modern Infrastructure

TRUSTED
Expert Advisory Services

RSA

Secureworks®

Dell EMC

vmware®
Pivotal®

virtustream®
A unified, phased approach to provide visibility, insights, and action to manage digital risk
THANK YOU!

Andy Waterhouse
EMEA Presales Director

Twitter : @Andy_J_W