EXECUTIVE SUMMARY
ALIGNING CYBERSECURITY WITH RISK
The agility and cost efficiencies associated with cloud, mobile and IoT are delivering on the business promises of disruptive technologies in IT operations. These trends, and the demands for regulatory compliance, need to be balanced with adequate controls and safeguards to ensure that risk exposure is being properly managed. The RSA™ Risk & Cybersecurity Practice provides a portfolio of advanced services that enables organizations to reduce risk by aligning security programs with business objectives.

Organizations seeking to identify gaps, improve readiness, evaluate risk, meet compliance and rapidly respond to incidents can take advantage of the RSA portfolio of advanced services:

- Battle-tested security consultants with over 35 years of experience delivering cybersecurity, identity, fraud and risk management solutions
- Global presence, delivering on up to 1,000 engagements on any given day
- Trusted by 370 Fortune 500 companies and 48 Fortune 50 companies

METHODOLOGY AND APPROACH
A HOLISTIC FRAMEWORK FOR END-TO-END SOLUTION FULFILLMENT
RSA addresses the lifecycle of solution fulfillment, from Strategy & Design to Deployment & Operations Management. The combination of technology and advisory expertise enables RSA to develop a holistic assessment of cybersecurity needs, reduce risk and rapidly respond to incidents.

Additionally, RSA provides a range of consulting services to address the “people, policy and process” aspects of a security program.

The RSA Risk & Cybersecurity Practice helps customers optimize their investments in RSA product platforms. RSA partners with these customers on the journey to fulfill end-to-end security program and risk management requirements, within a holistic and integrated Solution Fulfillment Framework.

RSA Solution Fulfillment Framework
Services portfolio ranging from requirements analysis and solution design to deployment and go-forward solution management
The RSA Risk & Cybersecurity Practice is aligned across key customer requirements with battle-tested consulting expertise in the following domains:

- RSA Risk Management Practice
- RSA Threat Detection & Response Practice
- RSA Identity Assurance Practice
- RSA Fraud & Risk Intelligence Practice
- RSA Incident Response Practice
- RSA Advanced Cyber Defense Practice

**RSA RISK MANAGEMENT PRACTICE**

**ENTERPRISE PROGRAM DEVELOPMENT**

Risk management programs empower organizations to efficiently implement risk management processes to significantly improve their business risk management maturity. Our practitioners provide industry expertise and best practices to design proven, multidisciplinary risk management solutions in the most efficient manner. Services include:

- **RSA Archer Platform Strategy & Roadmap**—designed to identify the elements required for the foundation of a holistic risk management program, targeting early wins while also developing longer-term strategy.

- **Cyber Risk Quantification**—work with FAIR certified consultants, leveraging the RSA Archer Cyber Risk Quantification Use Case, to quantify your organization’s financial risk exposure to cybersecurity events.

<table>
<thead>
<tr>
<th>Preliminary Use-Case List</th>
<th>Discovery Session Use-Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laws &amp; Regulations</td>
<td>Regulatory Sourcing</td>
</tr>
<tr>
<td>Interpretation</td>
<td>Regulatory Review / Applicability</td>
</tr>
<tr>
<td>Applicability</td>
<td>Regulatory Mapping</td>
</tr>
<tr>
<td>Business Process Mapping</td>
<td>Regulatory Change Roll-Out</td>
</tr>
<tr>
<td>Change Management</td>
<td>Change Management Sourcing</td>
</tr>
<tr>
<td>Impact Analysis</td>
<td>Enterprise Compliance Impact Analysis</td>
</tr>
<tr>
<td>Gaps</td>
<td>Business Unit Implementation Plan</td>
</tr>
<tr>
<td>Implementation</td>
<td>Compliance Liaison Reporting</td>
</tr>
<tr>
<td>Control Library</td>
<td>Controls Catalog Generation</td>
</tr>
<tr>
<td>Business Self Assessment</td>
<td>Controls Classification</td>
</tr>
<tr>
<td>System Control</td>
<td>Controls Mapping</td>
</tr>
<tr>
<td>Process Controls</td>
<td>FOPPs: SOP, Desk Guide Decomposition</td>
</tr>
<tr>
<td>FOPPs</td>
<td></td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>Risk Categorization</td>
</tr>
<tr>
<td>Regulatory Risk Assessment</td>
<td>Risk Register</td>
</tr>
<tr>
<td>Inherent and Residual</td>
<td>Regulatory Risk Assessments</td>
</tr>
<tr>
<td></td>
<td>Risk Appetite Program Tie-In</td>
</tr>
<tr>
<td>Testing &amp; Monitoring</td>
<td>Control Scoping</td>
</tr>
<tr>
<td>Validation of Processes</td>
<td>Control Testing (Attribute / Workpaper)</td>
</tr>
<tr>
<td>Transaction Testing</td>
<td>Compliance Reporting</td>
</tr>
<tr>
<td>Sampling</td>
<td>Continuous Controls Monitoring</td>
</tr>
</tbody>
</table>

**RSA Enterprise Risk Management Program Strategy**

Findings Report with use cases designed to align the security program with business requirements.
RSA THREAT DETECTION & RESPONSE PRACTICE
GETTING AHEAD OF THE THREAT
SIEM solutions enable organizations to aggregate and manage log data, often for compliance purposes. RSA provides customers with the ability to complement their signature-based detection capabilities with signature-less network and endpoint anomaly detection, all within the RSA NetWitness™ platform. Services include:

- **Use Case Development for RSA NetWitness**—the top threats to the organization (e.g., ransomware) are identified and the logic for detection is developed along with step-by-step response procedures for incident lifecycle management.

RSA IDENTITY ASSURANCE PRACTICE
ENTERPRISE IDENTITY MANAGEMENT
Identity is the core of all security programs and represents the most consequential threat vector in today’s fast-changing business environments. RSA identity assurance consultants can help with the most complex governance, lifecycle and multi-factor authentication challenges and also help to define and plan your identity and fraud programs to reduce the risk of tomorrow’s threats.

RSA has been working with customers for over 30 years as a leading provider of identity assurance solutions. Services include:

- **RSA Identity Assurance Strategy**—critical assets, privileged users and users with higher exposure levels (e.g., remote users and partners) are reviewed to align control requirements with risk propensity levels. Systems reviewed include Identity & Access Management, Enterprise Resource Planning, Customer Resource Management, Enterprise Content Management and technologies such as PKI, TLS, RADIUS, TACACS, LDAP and web-based single sign-on.

**RSA Identity Assurance Strategy & Roadmap**
Findings Report identifying critical assets for risk mitigation with RSA two-factor and risk-based authentication solutions
RSA FRAUD & RISK INTELLIGENCE PRACTICE

CYBERCRIME PREVENTION EXPERTISE

RSA is a leading provider of web and mobile solutions with expertise in advanced cybercrime threat prevention. Consumer solutions in particular need to be user friendly and convenient, without compromising security. Services offered include:

- Risk Account Manager—hands-on support and expertise for the RSA Adaptive Authentication platform, extended over a 12-month period, which enables fine-grained tuning of fraud rules and alerts for more effective fraud prevention and detection.

RSA INCIDENT RESPONSE PRACTICE

EARLY DETECTION AND RAPID RESPONSE

There's a narrow window of opportunity to prevent an adversary from carrying out his objectives after establishing a foothold in an organization. A well-designed Incident Response plan, combined with RSA IR Retainer services backed by on-demand cybersecurity experts, can make all the difference to breach mitigation. Engagements typically leverage the RSA NetWitness platform for packet capture and endpoint analysis and include:

- Proactive Incident Discovery/Compromise Assessment & Rapid Response—designed to detect the types of vulnerability that enable threat actors to bypass traditional defense mechanisms and assist customers with proactive threat detection and IR remediation.

- IR Retainer Portfolio—a variety of service-level options are available to provide customers with surge access to RSA IR expertise, enabling them to rapidly respond to an incident before harm is done to the organization.

---

Table of Contents

1 BACKGROUND
2 PROJECT OVERVIEW
2.1 INCIDENT DISCOVERY SCOPE AND METHODOLOGY
3 EXECUTIVE FINDINGS SUMMARY
3.1 Prevention Summary
3.1.1 High Risk Finding
3.1.2 Low Risk Finding
4 INCIDENT DISCOVERY DETAILED FINDINGS
4.1 Network Protocols
4.1.1 High - Consumed Protocols
4.1.2 Medium - Consumed Protocols
4.1.3 Medium - Exposed Protocols
4.1.4 Passive Network Detection: Suspicious Outbound Volume
4.1.5 Passive Network Detection: Suspicious Port Detection
4.1.6 Passive Network Detection: Time-Stamping
4.1.7 Passive Network Detection: Heuristics
4.2.1 Protocol Analysis of Scheduled Space and WMI Payloads
4.2.2 Alert - Cyber Espionage
4.2.3 Medium - Cyber Espionage Software
4.2.4 Medium - Cyber Espionage Tools
4.2.5 Medium - Cyber Espionage Malware
4.2.6 Medium - Cyber Espionage Technology
5 RECOMMENDATIONS
5.1 INCIDENT DISCOVERY INVESTIGATION RECOMMENDATIONS
5.1.1 General Tools
5.1.2 Outbound EDR and DLP Tools
5.1.3 Endpoint Agents
5.1.4 Access & Domain DNS Proxies
5.1.5 Access Domain Servers
5.1.6 Compromised Systems/Network Access
5.1.7 Compromised Systems/Network Access
5.1.8 Malicious/Non-Satisfactory Communications
5.1.9 Out-of-Date Software
5.1.10 Staging/Interception
5.1.11 Vendor & Analysts
5.1.12 SSL Traffic
6 APPENDIX A: DOCUMENTS REVIEWED
7 APPENDIX B: DISCOVERED NETWORKS
8 APPENDIX C: DISCOVERY TOOLS ARCHITECTURE
9 APPENDIX D: HOST FORENSIC ANALYSIS

RSA Incident Discovery

Findings Report table of contents for an engagement where the RSA NetWitness Platform is used to identify network and endpoint anomalies, which bypass traditional signature-based defenses.
RSA ADVANCED CYBER DEFENSE PRACTICE
READINESS AND RESILIENCE
Organizations need to know whether they are spending in the right areas and allocating scarce resources efficiently and effectively. RSA battle-tested Advanced Cyber Defense (ACD) experts enable organizations to identify gaps, prioritize risks and design an operational program to systematically improve defenses, integrate solutions, provide deep visibility, detect advanced threats and reduce mitigation time. Services offered include:

- **Strategy & Roadmap**—designed to identify gaps in current and targeted state maturity levels with comparison against peers for performance benchmarking.

- **Controlled Attack & Response Exercise**—to review and stringently test the response capabilities of the incident response team. In a controlled attack scenario, ACD designs and conducts several “capture-the-flag” exercises based on the customer’s existing toolset and IR processes and procedures. Results are scored based on flag difficulty levels and reviewed with the customer to identify areas for improvement.

- **SOC Services**—development of technical and operational specifications and capabilities for SOC Design & Implementation, including the use cases, incident response and threat intelligence programs, staffing and resourcing models and the step-by-step runbooks required to respond to incidents.

RSA PROFESSIONAL SERVICES
PRODUCT AND TECHNOLOGY DEPLOYMENT EXPERTISE
Each of the product practices provides professional services that help organizations optimize their investments in RSA technology platforms including:

- **RSA Archer™**
- **RSA NetWitness**
- **RSA SecurID™ Access**
- **RSA Identity Governance & Lifecycle**
- **RSA Adaptive Authentication**
- **RSA Web Threat Detection**

Each practice supports a holistic service portfolio that includes services designed to accommodate differing requirements and maturity levels:

- **Design and Implementation services**—to get the solution up and running, achieve “early wins” and accelerate time to value.

- **Subscription services**—used annually to progress the maturity of the solution and work hand in hand with the customer to identify and implement use case requirements and enhance overall solution effectiveness.

- **Tuning & Optimization services**—recommended annually to maximize and tune solution performance, upgrade the environment to the latest release and implement additional features and functions.

- **Product Integration services**—to accommodate the integration of RSA products with third-party products and IT systems, such as IT ticketing.
• **Custom services**—tailored consulting for platform migrations, technology integration, high-availability configurations, residencies and “expert-on-demand” staff augmentation.

• **Offshore services**—lower-cost solution fulfillment by the RSA Virtual Services Delivery (VSD) team.

**RSA UNIVERSITY**

**CYBERSECURITY & RISK MANAGEMENT TRAINING PROGRAMS**

RSA provides a combination of on-demand and instructor-led training to ensure that customers can enhance overall awareness, maximize the return on their product investments and optimize their cybersecurity capabilities.

The RSA Certification Program provides technology professionals with the knowledge, skills and credentials needed to deploy and manage RSA enterprise security systems. Several certification exams are available for each suite of products. Other courses offered by RSA University include Security Awareness Training and boot camps for the CISSP and Certified Ethical Hacker certifications.

**PUTTING IT ALL TOGETHER**

**ENTERPRISE-WIDE RISK MANAGEMENT**

Protecting an organization’s critical assets requires the right combination of technology and expertise. The RSA Risk & Cybersecurity Practice represents a team of battle-tested security practitioners who are delivering solutions at scale on a global basis. When combined with the RSA industry-leading technology portfolio, organizations can avail of embrace the opportunities agility and efficiency presented by the latest development in IT while managing the risks to their business.

**ABOUT RSA**

The RSA provides more than 30,000 customers around the world with the essential security capabilities to protect their most valuable assets from cyber threats. With RSA Global Services’ capabilities and award-winning products, organizations effectively detect, investigate and respond to advanced attacks; confirm and manage identities; and ultimately, reduce IP theft, fraud and cybercrime.

Education services are available from RSA University, and product maintenance and Personalized Support Services are available from RSA Customer Support. For more information, go to [rsa.com](http://rsa.com).

©2018 Dell Inc. or its subsidiaries. All rights reserved. RSA and the RSA logo, are registered trademarks or trademarks of Dell Inc. or its subsidiaries in the United States and other countries. All other trademarks are the property of their respective owners. RSA believes the information in this document is accurate. The information is subject to change without notice. 04/18, Data Sheet, H15836.