Document Library Executive Summary

The March 2011 attack against RSA Security was a devastating blow to the company, costing the firm $66.3 million in an immediate quarterly earnings charge, forced a reissuing of hardware to over 30,000 customers, was directly tied to leaks of classified documents from our clients, and was a major blow to the credibility of the firm. The initial incident was initiated by an employee falling victim to a phishing email which began a series of compromises that eventually spanned multiple continents and resulted in the loss of our crown jewel technology.

Subsequent analysis of the incident has identified both successes and opportunities for improvement in the company’s cybersecurity posture. The goal of this document library is to demonstrate RSA Security’s commitment to moving forward by presenting historical reports, updated process documents, and testing results, including:

1. A compendium of incident response terms and definitions, which may be utilized in new and future documentation (TermsandDefinitions)
2. An updated Incident Response Plan and follows the NIST 800-53 Incident Response standard (IncidentResponsePlan)
3. One of our new Incident Response playbooks that demonstrates our attention to standardization during an incident response action (Incident\_Response\_Playbook)
4. The threat hunting checklist that is in use by our new Security Operations Center global threat hunting team (Threat\_Hunting\_Checklist)
5. Our threat intelligence feed using a heat map for analysis (ThreatIntelHeadMap), as well as a mapping of the identified attacker (APT1) to the MITRE ATT&CK (Threat\_Intel\_MITRE-ATTACK)
6. The results of our latest leadership-level tabletop exercise (Tabletop\_Exercise)
7. The SIEM use cases which are being leveraged for the evaluation and acquisition of the new global SIEM solution (SIEM\_Use\_Cases)
8. The Incident Investigation Report that was generated as a result of the original 2011 attack (Incident\_Investigation\_Report)
9. The updated Incident Response Communication plan that has been recently implemented to ensure that leadership is notified during a Severity 1 incident (IncidentResponsePlan)
10. Position descriptions and skills/certifications expectations of our new Security Operations Center personnel. (SOC\_Job\_Categories)

We believe these documents will evidence of our commitment to advancing our security posture and continuing to defend against the espionage that has targeted our intellectual property.

Thank you.

RSA Security Leadership