

# RSA® ARCHER® INCIDENT MANAGEMENT

## Anwendungsbeispiel für Business Resiliency

### Die Herausforderung

Die Reportinganforderungen an Berichte zu Betrugs- und Cybervorfällen sowie Whistleblower- und physischen Sicherheitsbedrohungen werden durch verschiedene Bestimmungen (z. B. Public Disclosure Act, Sarbanes-Oxley Act) vorgegeben. Viele Unternehmen haben Prozesse zur Reaktion auf Vorfälle für Geschäftseinheiten oder Standorte erarbeitet. Häufig werden diese Prozesse manuell implementiert und über Tabellenkalkulationen oder selbst entworfene Lösungen gemanagt. So werden wertvolle Zeit und Ressourcen darauf verwendet, Vorfälle nachzuverfolgen, anstatt sie zu beheben.

Wenn einfache Incidents zu Geschäftsunterbrechungen oder gar Krisenereignissen führen, können sie den Betrieb ernsthaft beeinträchtigen und sich negativ auf die Compliancefähigkeit, die Finanzen und den Ruf Ihres Unternehmens auswirken. Unternehmen benötigen ein zentrales Repository mit Tools zur Unterstützung von Echtzeitentscheidungen, mit denen Mitarbeiter im Fall von Ereignissen, die sich auf Mitarbeiter, Kunden, den Betrieb oder den Ruf der Marke auswirken, schnell und effektiv reagieren können.

### Übersicht

**RSA® Archer® Incident Management** bietet ein vollständiges Fallmanagementsystem zur Berichterstattung über Cyber- und physische Incidents sowie deren Kategorisierung und der Bestimmung der geeigneten Vorgehensweise. Sie können die Wichtigkeit eines Incidents bewerten und basierend auf den Geschäftsauswirkungen und den behördlichen Auflagen Mitglieder des Reaktionsteams zuweisen. Incident Management bietet ein Dashboard mit Kennzahlen zum Nachverfolgen und Reporting von Kosten, verwandten Incidents, Verlusten und Recovery.

### Hauptmerkmale

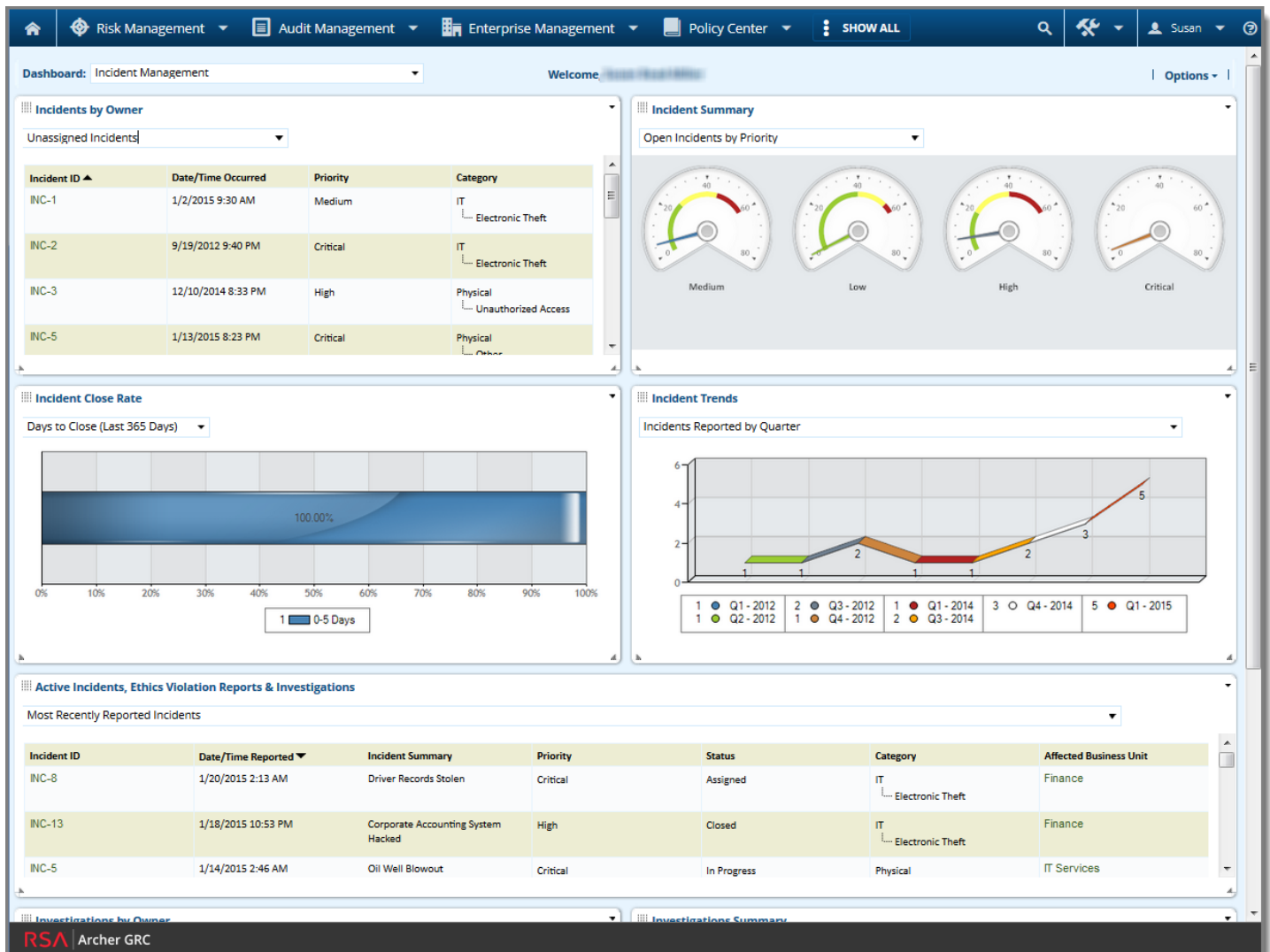
- Zentrales Repository zum Reporting von Incidents und Management des Incident-Lebenszyklus
- Zentrales Repository für Kontaktinformationen für Incident-Ermittler, Zeugen und andere an der Ermittlung beteiligte Personen
- Liste der behobenen Incidents nach angefallenen Kosten
- Hinterlegen aller Verfahren, die bei Auftreten von Incidents implementiert werden müssen, nach Incident-Art (Denial of Service, Phishing-Angriff uvm.) kategorisiert

### Die wichtigsten Vorteile

Vorzüge von RSA Archer Incident Management:

- Zentralisieren von Incident-Daten, Melden durch Anwender von Cyber- und physischen Vorfällen jeglicher Art, einschließlich Diebstahl, Belästigung, Betrug und Phishing

- Anonymes Melden von Incidents durch Whistleblowers und Integrieren von Daten eines Callcenters oder eines Services zum Erkennen von Angriffen über die flexible Archer Web Services API
- Kontrollierter Zugriff auf Incident-Daten bis zur einzelnen Feldebene, um die Identität der beteiligten Einzelpersonen und die Integrität der vertraulichen Daten Ihres Unternehmens zu schützen
- Verknüpfen von Incidents mit spezifischen Ergebnissen und Maßnahmenplänen sowie Überwachen aller Eindämmungsmaßnahmen und -genehmigungen
- Erstellen von Rollup-Berichten zur Nachverfolgung von Incidents und Identifizierung von Trends, Ähnlichkeiten von Incidents und Beziehungen



## Weitere Informationen

Weitere Informationen darüber, wie Produkte, Services und Lösungen von EMC Sie bei der Bewältigung Ihrer Geschäfts- und IT-Herausforderungen unterstützen, erhalten Sie von Ihrem Vertriebsmitarbeiter oder autorisierten Reseller vor Ort oder auf unserer Website unter [www.rsa.com](http://www.rsa.com). Wenn Sie bereits Kunde von RSA Archer sind und Fragen haben oder zusätzliche Informationen zur Lizenzierung wünschen, wenden Sie sich bitte an RSA Archer unter [archersupport@rsa.com](mailto:archersupport@rsa.com) oder rufen Sie die Nummer 00800 772 49000 an.

EMC<sup>2</sup>, EMC, das EMC Logo, RSA, das RSA-Logo und Archer sind eingetragene Marken oder Marken der EMC Corporation in den USA und anderen Ländern. VMware ist eine eingetragene Marke oder Marke der VMware, Inc. in den USA und anderen Ländern. © Copyright 2016 EMC Deutschland GmbH. Alle Rechte vorbehalten. Veröffentlicht in Deutschland. 4/16 Datenblatt H14792-1

RSA ist der Ansicht, dass die Informationen in dieser Veröffentlichung zum Zeitpunkt der Veröffentlichung korrekt sind. Die Informationen können jederzeit ohne vorherige Ankündigung geändert werden.

**RSA**  
www.rsa.com