RSA® ARCHER® INCIDENT MANAGEMENT

业务弹性的使用情形

挑战

多项法规要求提供有关欺诈、网络事件以及告密者和物理安全威胁的报告，包括公共信息披露法案和 Sarbanes-Oxley 法案。许多组织已经针对各业务部门或位置制定了事件响应流程，这些流程通常手动实施，并且通过电子表格或自主开发的解决方案进行管理。因此，将宝贵的时间和资源用在了跟踪事件上，而不是解决事件上。

当简单的事件演变为业务中断或危机事件时，它们可能对贵组织的运营、法规遵从性能力、财务和声誉造成严重危害。公司应该有一个实时决策支持工具的中央存储库，这些工具使工作人员在发生影响到员工、客户、运营或品牌声誉的事件时，能够快速有效地做出反应。

概述

RSA® Archer® Incident Management 提供案例管理和事件响应，以报告网络和物理事件、将其加以分类并确定相应的响应程序。您可以基于业务影响和监管要求评估事件的关键性并分配响应团队成员。Incident Management 还提供指标控制面板来跟踪和报告成本、相关事件、丢失和恢复。

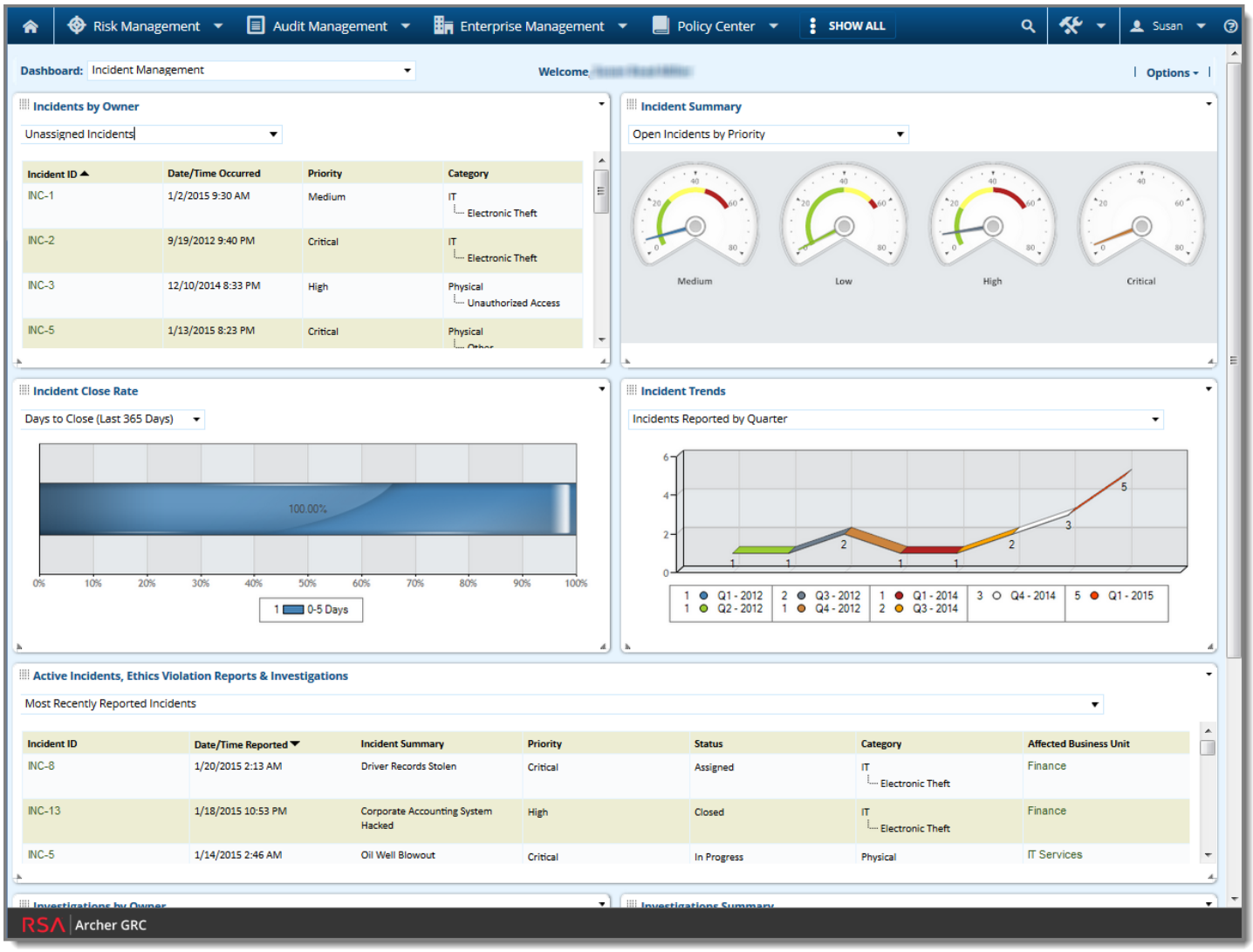
关键功能

- 用于报告事件和管理事件生命周期的中央存储库
- 包含事件调查者、证人以及参与调查流程的其他人员的联系信息的中央存储库
- 按解决成本分类的已解决事件的列表
- 包含在事件发生时必须实施并按事件类型（拒绝服务、网络钓鱼攻击等）分类的所有程序的存储库

主要优势

借助 RSA Archer Incident Management，您将能够：

- 集中事件数据，并允许终端用户报告任何类型的网络和物理事件，包括盗窃、骚扰、欺诈和网络钓鱼
- 允许告密者匿名报告事件，以及通过灵活的 Archer Web Services API 整合来自呼叫中心或入侵检测服务的数据
- 控制对深入到单个字段级别的事件数据的访问，以保护参与人员的身份信息和贵组织机密信息的完整性
- 将事件关联到特定的调查结论和补救计划，并监控所有补救措施和批准
- 生成汇总报告以跟踪事件并确定趋势、事件相似处和关系



了解更多信息

如欲详细了解 EMC 产品、服务和解决方案如何帮助您解决业务和 IT 难题，请联系当地销售代表或授权经销商，或者访问我们的网站：www.rsa.com。如果您是现有的 RSA Archer 客户并遇到了问题或者需要有关许可的其他信息，请通过 archersupport@rsa.com 或致电 (8610) 8438 6000 联系 RSA Archer。

RSA
www.rsa.com