

AT&T Consulting

Incident Management Program Security Services

Incident management aims to prevent or minimize operational losses due to undesired operational events. Aside from providing a tangible operational and financial benefit to your organization, a comprehensive incident management program may be a regulatory requirement for organizations in certain industries, as well as a key part of industry standards and best practices. The AT&T Incident Management Program service provides expert resources to assess and improve any or all stages of your incident management lifecycle; from assessment of the existing program, to optimization of existing tools and processes, development of metrics and actuarial records or a complete overhaul. AT&T Consulting will create custom solutions that are practical, efficient and help address regulatory compliance requirements.

Incident Management

Incident management has transformed significantly during the past decade. Perhaps the most significant change has been the shift in focus – from a reactive response to a proactive, preventative approach. Although new technology solutions, such as Intrusion Prevention Systems (IPS), Security Event Management (SEM) and others have enabled the new proactive approach, the evolving threat landscape, the ever-increasing complexity of current technology solutions and lack of “horizontal” integration of incident management processes are significant challenges in many organizations. The common approach of meeting only the minimum regulatory requirements has limited both the development and results of incident management programs. The lack of adequate incident metrics and actuarial (loss) data has hindered implementation of overall technology risk management programs.

Solution

AT&T Consulting can provide a broad range of services aimed at assessing and improving incident management programs. The main solutions within the AT&T Incident Management Program services consist of:

- Incident Management Program Assessment
- Incident Management Strategy and Roadmap Development
- Incident Response Plan and Playbooks/ Scenarios Development
- Incident Management Training
- Incident Response Testing and Evaluation

Incident Management Program Assessment

AT&T Consulting will review all relevant documentation, observe daily incident management activities and review previous incident management reports and metrics. This also includes the existing incident management framework, the touch-points and integration of incident response activities with other IT and non-IT operational processes (such as risk, threat, and vulnerability management), and existing MSSP interactions. AT&T also assesses the adequacy of the technology solutions supporting incident management activities (feature and implementation). AT&T Consulting will use its leading-edge, custom developed incident management framework and applicable regulatory requirements for performing the gap analysis and proposing practical remediation recommendations for technology and cultural realities. A Software Engineering Institute Capability Maturity Model (SEI-CMM) based assessment of the maturity level of key components of the existing incident management program can also be included in the assessment.

Benefits

- Proactive approach to data breach prevention
- Helps mitigate security risk through proactive measures
- Delivers a comprehensive incident response plan and ongoing support to help organizations respond in case of a security incident
- Provides on demand security expertise on preparing for and responding to incidents
- Provides comprehensive risk mitigation support
- Stops attacks in progress to mini-mize their impact
- Improves incident response preparedness

Features

- Incident Management Program Assessment
- Incident Management Strategy and Roadmap Development
- Incident Response Plan and Playbooks/Scenarios Development
- Incident Management Training
- Incident Response Testing and Evaluation



Incident Management Strategy and Roadmap Development

AT&T Consulting will use the results of the gap assessment and its analysis of the threat landscape relevant to your organization to develop a “desirable”, future state for your incident management program. A pragmatic roadmap between the current and the future state will be created. The roadmap will provide detailed descriptions of all relevant technology, process, and people components, tasks, dependencies and milestones. Metrics will be created to track progress and support a future state of continuous improvement.

Development of Incident Response Plan and Playbooks

AT&T can develop a custom incident response plan (and associated operational processes) for your organization based on the threat, regulatory, organizational and cultural and technology realities. Our methodology emphasizes prevention, accurate detection and identification, practical triage and prioritization, response processes integrated with overall IT service and risk management processes and comprehensive reporting and metrics. Practical playbooks can be developed for incidents most likely to be encountered.

Incident Management Training

AT&T Consulting can improve your incident management program through knowledge-transfer sessions and custom training development and delivery for all your representative stakeholders (from executive staff to incident response coordinators and handlers). Our workshops can provide training and insight into general incident management matters or specific scenarios. For example, AT&T consultants can demonstrate the use of the incident management plan for responding to potential incidents, present lessons learned from our experience providing real-world incident response services and perform post-mortem analysis from previous incidents.

Incident Response Testing and Evaluation

AT&T Consulting can provide a practical validation of an existing or newly updated incident response plan and playbooks through simulated incident response exercises. These exercises will assess the real-world effectiveness of the updated incident response plan or playbooks and identify opportunities for further optimization. AT&T staff can either monitor the exercise or perform the actual response activities.

Simulated incident response exercises are also excellent for knowledge transfer and training for your staff. AT&T simulated exercises are designed to meet relevant requirements, such as PCI.

Key Benefits

AT&T Consulting takes a holistic approach to Incident Management, addressing elements of people, technology and processes. We combine in-depth knowledge and use of Information Security Standards of Good Practice, applicable regulatory requirements and our experience in information security management practices within the industry.

Security Solutions: Expertise from a Trusted Provider

AT&T provides a unique and world-class portfolio of compliance and related security services. Our experience, expertise and commitment to open standards have established us as a strategic and trusted advisor. By leveraging AT&T you can expect best-in-breed solutions, a global network of proven technology, and a cost-effective program-based approach to meet your compliance needs.

For more information, contact an AT&T Representative or visit us at www.att.com/consulting/security.