Responding to Security Incidents: A Collaborative Approach
Vijayaraghavan Raghu
Solution Architect – IT Infrastructure Services

Vijayaraghavan Raghu is Solution Architect with TCS’ IT Infrastructure Services, with specific focus on Enterprise Security. He is currently responsible for strategic solutions design and pre sales support. In his 14-year long career with TCS he has been the Security Practice / CoE head and has also managed delivery for key clients in the Banking and Retail industries. He is accredited with CISA, CISSP and CCSK certifications.
With the advent of integrated IT products and converging technologies, it is critical for IT organizations to adopt a holistic view of IT security operations and support, and their impact on the enterprise. They need to be aware of the critical role that applications, infrastructure and security play in response to any threat to confidential data. In addition, organizations need a reliable strategy to efficiently manage persistent issues surrounding orchestration, participation and implementation of processes for security incidents and threat responses.

This paper focuses on enabling IT organizations to identify the right engagement model that will help foster a collaborative approach among various functions within the organization when responding to IT security incidents.
Contents

1. Introduction 5
2. Challenges in Engaging IT Support 5
3. Achieving Effective Engagement 6
4. Establishing a Simple Engagement Model 7
5. Creating Collaborative and Responsive Teams 7
6. Developing an Operations Responsibility Map 8
7. Conclusion 9
1. Introduction

The increasing focus on regulatory compliance and maintaining global industry operational standards is driving organizations to conduct periodic security testing. The security tests are conducted to validate the process and the procedures to respond to any incident. Generally, these help in validating roles and participation of various teams and ensure preparedness. However, in reality these tests are carried out in silos by separate teams to monitor, support operations and security emergency response, while IT support is called only to resolve any issues or respond to emergency situations. But efficient and effective response to security threats and incidents calls for a consistent engagement of IT security as well as the operations teams, and a synergistic management of change across the enterprise.

2. Challenges in Engaging IT Support

Technology support for business is increasingly being integrated and automated. Furthermore, the data and systems are being moved to cloud providers to achieve greater ROI and improved availability. This is pushing business and IT management functions to adopt innovative products, solutions and services that are pre-packaged and ready to deploy.

As security incidents attract high visibility, security teams are under tremendous pressure to respond quickly to change and Innovate by making effective and on-time updates to security management systems. However, with the rapid pace of change, security teams often have to deal with reduced cycle times to prepare and address security risks associated with new and emerging technologies.

Additionally, most organizations do not have a clear definition of a security incident. They fail to identify the potential impact of a threat or risk of an incident on the business. As a result, they are left with inadequate resources to respond to such an event.

If the IT security team has to respond to a specific security threat effectively, it should successfully engage with the enterprise architecture, applications, network operations, datacenter and end point support. Traditionally, these functions or units have their own objectives and operational responsibilities aligned to the overall organizational goals. This bring up a unique challenge in effectively engaging all the teams and executing enterprise IT security plans and strategies.
3. Achieving Effective Engagement of All Functions

It is critical that IT organizations understand the requirements, priorities and challenges of security governance, and build an appropriate engagement model based on these factors. Organizations can gradually evolve such a model by addressing a few fundamental questions:

- What are the potential risks that the organization faces due to lapse in security?
- What are the mandatory regulatory and compliance requirements?
- What systems are in place to monitor security incidents?
- Who orchestrates the response to any security incident?
- Who is responsible and accountable for responding to IT security incidents?
- Who is engaged in managing the IT security such as application security, firewall, IDS/IPS, security tools, end point security and access provisioning?
- What level of engagement does IT Security have in the application development lifecycle?

A simple engagement model, as depicted in Figure 1, consists of three components – a focused security organization, a diversified model and a dedicated model. Each component displays different characteristics but can coexist in an organization depending on the scale and value of the information exchanged at various levels, as well as other parameters. It is a complex matrix, which presents several challenges related to shared responsibilities and incident response execution.

![Engagement models](image-url)
4. Establishing a simple Engagement Model

<table>
<thead>
<tr>
<th>Diversified</th>
<th>Dedicated</th>
<th>Focused</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT security infrastructure and process support within the IT support function</td>
<td>Independent team of IT security personnel</td>
<td>Security operations outsourced to security service provider, governed by focused dedicated internal security organization</td>
</tr>
<tr>
<td>All supporting functions report to IT operations support only</td>
<td>Security operations reports to IT security management</td>
<td>Shared responsibility between IT Security and other technology support teams with clearly defined responsible, accountable, consult and inform (RACI) matrix</td>
</tr>
<tr>
<td>Limited segregation of duties</td>
<td>Security operations shares responsibility with other IT groups and has a clearly defined RACI matrix</td>
<td>Driven by policies and procedures</td>
</tr>
<tr>
<td>Low sensitivity to security needs</td>
<td>Based on clear segregation of duties</td>
<td>Documented and audited segregation of duties.</td>
</tr>
<tr>
<td>Efforts dedicated to address minimal compliance requirements</td>
<td>Holistic approach that goes beyond compliance needs</td>
<td>High sensitivity to security needs; requires dedicated Chief Information Security Officer</td>
</tr>
</tbody>
</table>

5. Creating Collaborative and Responsive Teams

Organizations require structured IT governance that adheres to corporate policy and consistently evolves with changing goals and business challenges. IT security must be a top-down process and CXOs must be completely aligned with the strategies and policies. But the execution of those policies must be bottom-up. It is at these tactical and operational levels that organizations can face inherent challenges compounded by lack of or slow communication, training and flow of information to all relevant individuals. The top management’s focus and investment of time and dedication also influences the security competency of an organization.

A good starting point is to build a robust roadmap towards shared responsibility for operations support and security incident response. This can be facilitated by designing an operations responsibility map (ORM), which defines the sharing of responsibilities between teams involved in security incidents, and keeps them well prepared to initiate a quick, collective and effective response to incidents.
6. Developing an Operations Responsibility Map

The key steps involved in preparing a smart operations responsibility map that can drive effective security incident response include:

- Listing all critical and possible activities in the event of an incident.
- Identifying the products and technology enablers to automate, correlate and respond to security events.
- Defining the coverage of security operations and identifying the key stakeholders to maintain the security posture.
- Outlining the security incident management process.
- Identifying the players in the IT organization that:
  - Monitor the specific IT infrastructure or platform components.
  - Manage the security monitoring and response technology, device or tool.
  - Support activities that enable the security operations teams to respond quickly and effectively.

By establishing these critical elements of the security framework, organizations can get a snapshot of the tactical landscape. Figure 3 illustrates a sample operations responsibility roadmap.

---

**Example**
- Network Security Device Monitoring & Management
- Content Filtering Administration
- Secure Access Control
- Wireless Security
- Vulnerability Management
- Penetration Testing
- Perimeter / DMZ Management
- Incident Response & Management

**Monitored By**
- Security Operations Center
- Network Operations Center

**Managed By**
- Network Operations Management Group
- Security Administration Group

**Supported By**
- Data Center Administrators
- Server Management Teams
- Security & Network Architecture Group
- Incident Management Team

**Operations Responsibility Map**

**Activities**

**Enabled By**

**Products / Tech**

**Support Team(s)**

**Monitored By**

**Managed By**

**Supported By**

---

**Figure 2: Security Incident Response – A sample operations responsibility map**
7. Conclusion

Though IT security has matured and moved beyond the peak of inflated expectations, there are challenges and issues for effective security. The solution lies in gaining a thorough understanding of the current IT organization, so that IT operations and security teams can collaborate effectively to meet all pressing security needs. This collective enterprise-wide approach results in clear communication and awareness of the policies and processes, and the sharing of responsibilities. This understanding must further be translated into a clear RACI chart with a sign-off from each managing stakeholder for sustained success. While clearly maturing beyond the Peak of Inflated Expectations, IT Security continues to be one of the most hyped subjects in IT. A perceived lack of security has been one of the more prominent reasons organizations cite for not adopting cloud services. However, this attitude is changing rapidly as IT service providers (ITSPs) begin to offer comprehensive security capabilities. Security and risk pros must accept that IT Security is here to stay and develop strategies to deal with this new reality. In the swift adoption of enterprise wise IT Security technology is sometimes an afterthought, an undertaking for which sufficient time and resources don’t exist. Tools such as operations responsibility map can help security professionals validate their approach to security and risk management controls by making sure they have not overlooked key areas of concern. Security and risk professionals must also develop strategies and collaborative teams to deal responsively with the security challenges associated with the swift adoption of emerging technologies.

As noted in the section on Engagement Models, understanding the current IT organization plays a key role in delving further to improve the participation of IT operations for security needs. This collaborative approach results in clear communication and understanding of the activities and the share of responsibilities.
About TCS IT Infrastructure Services

TCS IT Infrastructure Services (ITIS) practice is a strategic business unit of TCS providing you with effective infrastructure management solutions and transform your IT landscape by leveraging our expertise in next-generation models such as IaaS, PaaS, and SaaS. Our unique Global Network Delivery Model (GNDM™) allows you to choose the sourcing strategy best suited to run your business efficiently thus providing seamless experience across all operations.

TCS ITIS has established several Technology Centers of Excellence (CoEs) across various platforms and technologies to bring enhanced value in terms of technical support, knowledge management, training, continuous service improvement and innovation for our clients.

Our offerings are backed by the Assess-Build-Manage-Transform framework that leverages our partner eco-system, tools and automation framework, and Technology Centers of Excellence (CoEs). Spanning the entire scope spectrum of IT and infrastructure related needs, our offerings include End-User Computing (EUC) services, IT Service Desk, Converged Network services, Managed Security services, Application Management services, Enterprise Systems Management, IT Service Management, Data Center services, Mobility services, Cloud services and Transformational solutions.

Contact
To know about TCS PaaS Offering, contact itis.presales@tcs.com

Subscribe to TCS White Papers
Feedburner: http://feeds2.feedburner.com/tcswhitepapers

About Tata Consultancy Services (TCS)
Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match.

TCS offers a consulting-led, integrated portfolio of IT and IT-enabled infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India’s largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

IT Services
Business Solutions
Consulting