LEVERAGING INCIDENT MANAGEMENT FOR CONTINUAL IMPROVEMENT

GANESH VISWANATHAN,
SENIOR VP-PMO & CISO, AITHENT TECHNOLOGIES PVT. LTD.

AUTHOR'S BIO

Ganesh has over 30 years of experience in IT & Services and Engineering industry with diverse Management experience with specialization in IT Security, Risk & Compliance, Project Management, Strategic Planning and Supply Chain Management.

Ganesh is a Lead auditor in ISO 9001, and is trained in Project Management, Eli Goldratt's Theory of Constraints, six sigma & holds several Security Certifications. Ganesh holds a Bachelor's degree in Technology from Indian Institute of Technology, Madras.

Ganesh is currently working with Aithent as SVP-PMO & CISO since March'19. He last worked at Quattro for 12 years where he was **SVP-Chief Information Security & Privacy Officer** responsible for Cyber Security & Privacy and Quality.

He has developed 7 products for financial services and spearheaded the implementation of ISO 27001, SSAE 18, PCIDSS, Data Protection Act, 1998, GDPR & RBI regulations. He has won several awards in the Information security & Privacy space and has addressed several conferences as a key note speaker/panelist

INTRODUCTION:

Given the current threat landscape which is constantly mutating with arrival of new threat vectors and increasing sophistication of attacks; the volume of attacks is spiraling with low probability of detection, volatility of attacks is growing by the day, attacks come unannounced and they are in the system up to 6 months prior to the actual attack and are doing reconnaissance or scanning the network or are already exfiltrating the sensitive data or are erasing your files or the attackers are installing a backdoor as part of an exploit; cyber vulnerabilities are growing at a rapid clip; we have to develop an integrated and holistic approach to manage cyber incidents.

Planning is the sine qua non for an excellent execution. As the saying goes "By failing to prepare, you are preparing to fail". Develop a detailed Business Continuity Plan (BCP) to plan for various contingencies that arise out of multitude of threats so that regular Business can continue smoothly. For the Communications, hardware and IT systems which constitute the vital support systems, develop a Disaster Recovery (DR) plan. Make sure that the BCP/DR Plan it is communicated to all the stakeholders and a refresh training is conducted periodically.

To check readiness of employees in case of any emergency do a Call Tree testing at least once in 6 months. The employee contact list should be updated on a monthly basis for ensuring that the proposed call tree exercise in case of an actual disaster is accurate and meaningful. Resiliency testing of key services should be conducted at least annually to ensure a robust business continuity program. Besides do a quarterly

fire drill and appoint a fire marshal for each Floor shift wise. Do a periodic audit of your Fire preparedness. A mock drill needs to be carried out for Earthquake preparedness too. Employees should be educated about the Do's and Don'ts through posters, screen savers, class room training and regular email updates.

Critical network equipment such as routers, core switches and critical servers should also be subjected to a Disaster recovery (DR) testing. Every step of Disaster Recovery plan is tested as part of DR testing to check the timely restoration of business-critical applications, recovery of data and continuation of operations after a service interruption. DR Testing is an investment for the success of BCP. It gives us the confidence that the DR plan shall works as intended when deployed during an Emergency. The BCP plan is a live document and needs to be updated based on learnings from incidents/disasters. Ensure that hard copies of it are kept offsite to handle any emergency.

An incident is an event that could lead to loss of, or disruption to, an organization's operations, services or functions. Incident Management describes the activities to identify, analyze, and correct the occurrence of any disruptive event

Following are the steps to be followed for a successful Incident Management Program:

1. Detection: Identify all issues that emanate from Infrastructure monitoring tools be it memory, CPU, Disk space or Alerts from a Data Leak Protection (DLP) solution or Intrusion Prevention system (IPS) or a Firewall. Record user issues in terms of latency, response time, space availability. Record the voice of the user as he or she may detect unknown problems by Co Workers which could lead to potential information security incident such as Tailgating when entering the building premises or the Operations floor or Carrying mobile phones in a sanitized operations area where it is strictly prohibited. Sharing of passwords is also considered as an Incident. A whistle blower policy needs to be developed which will reinforce the appropriate code of conduct at work place.

Log all Incidents and identify the trends. Identify if the incident is a New or Recurring one to investigate ownership and responsibility.

Classify the incident as a Service related or Hardware or Software or Compliance (Not following laid out Policy or SOP by Employee)

Prioritize the incident in terms of severity as per the Severity matrix based on Impact, Urgency or Risk. Impact is high if large number of users are unable to use a service. Urgency is high if the service is critical to client and downtime will affect the business. Risk is high if a Fire suppressant system malfunctions in a Data center or the Precision AC fails, and temperature raises.

2. Diagnosis: As part of trouble shooting, investigate the root cause. Tools such as 5W, 1H can be deployed for a logical analysis. Identify Who was involved, What happened, Where did the incident happen, When did it happen, Why did it happen and How did it happen. Follow the Escalation procedure for cases where incident needs to be notified (client end) or resolved (In-house/Vendor) at a higher support level.

3. Resolve/Repair: Fix the issue by going for a temporary workaround or a permanent fix. In case it is a temporary fix the plan for permanent fix must documented along with any support (In terms of time, spare, additional resources etc.). The repair may involve replacing a part (hardware) or Uninstalling the infected software. Installation of a fresh patch/ latest version of the software /Running an Anti-Virus software/Rebuilding OS or a simple configuration change (software) or following a new SIPOC (Process map)/SOP. This may also involve a coordinated shutdown of associated parts, wiping the infected devices and rebuilding the Operating system.

4. Recovery: It entails Service restoration or a System (Network) Validation. New Passwords must be created for all the compromised systems.

5. Documentation, Follow-up & Closure: Once the correction is completed document the findings in an Incident Report detailing all the steps followed. This will help prevent recurrence of the incident. Carry out a review to determine if the detection was without any delay, if the preparations were adequate and if cross functional support was timely. Monitor activities post incident to check if the threat vectors are reappearing which may cause the incident to reoccur. Post this the Incident can be formally closed.

Conclusion: By following the five steps in the Incident Management Framework as part of Incident Response, organization will reap the benefits through continual improvement in the client SLA's and key Security Metrics. It will act as a springboard to defend the organization from both external and internal threats thus helping them to protect their digital assets. This structured methodology will make the Cyber security robust, resilient and reliable thus validating the proverb "An ounce of prevention is worth a pound of cure".