Simulation of Mock Drills in Cyber Security

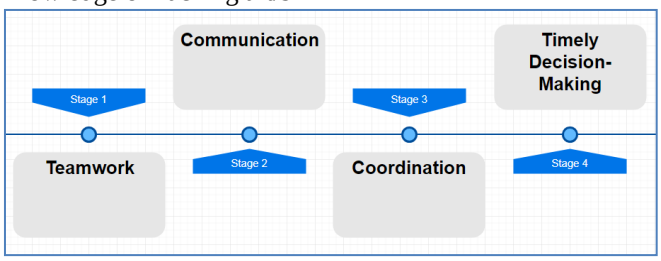
Ashish Yadav
Department of Information Technology
CERT-India

Abstract— Over the years, Information Technology has transformed the global economy and connected people and markets in ways beyond imagination. The government is also encouraging financial institutions, industry and other critical sectors to earmark higher budgets in line with the international practices towards development and implementation of appropriate technologies, as well as bringing forth best practices for protecting their information and communication technologies.

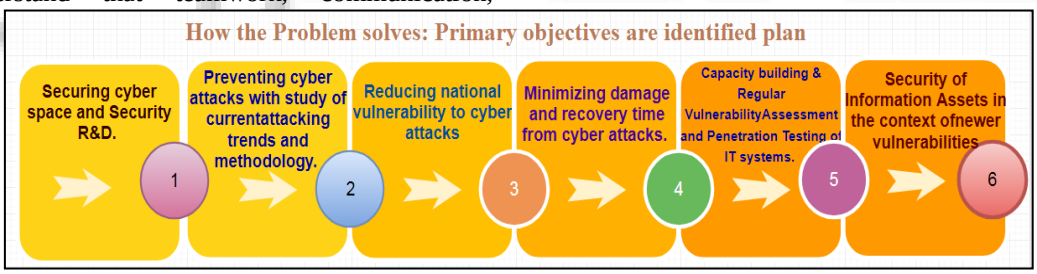
Key words: Cyber Security, Information Technology

I. The Problem

Information technology from a security/defensive point of view, it comes to classify/evaluating technology in preparation for a probable disaster or cyber security incident, IT security departments routinely conduct multiple tests, run out different scenarios to see how applications, systems, devices, and interfaces will respond in the event of an outage or attack. In business continuity, emergency management, or disaster recovery outlining tests, instability in backup processes and failover procedures are spotlighted when systems go offline and critical data is unavailable. The Solution Design: In this paper I am taking about testing your people? For example, how would your IT or security team respond to a recent massive ransomware attacks, or to a strategic DDoS assault? The reality is that security team preparation and readiness or lack of it is often more of a problem than the technology. So, Exercise participates experts understand that teamwork, communication, coordination and timely decision-making are tested in these cyber security incidents presumably even more than knowledge or hacking art/skill

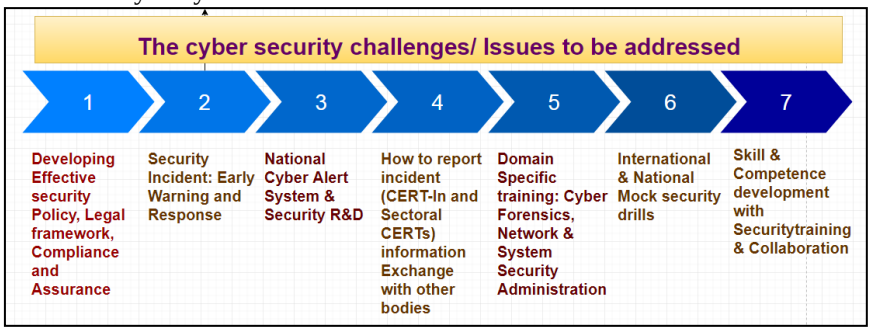


The Solution Design: In this paper taking about testing your people? For example, how would your IT or security team respond to a recent massive ransomware attacks, or to a strategic DDoS assault? The reality is that security team preparation and readiness or lack of it is often more of a problem than the technology. So, adopting an attacker's mindset can effectively help businesses enhance their chances of securing themselves against ever-changing threats. Playing the role of an attacker can make your team better at defense. Learn how in our step-by-step guide to cyber security mock drill your security infrastructure from involving the right people to a hypothetical vs live event. The military, government offices and the national security agencies all following this concept of Mock Drills. The concept has made its way into the corporate world like/e.g.: war-gaming the security infrastructure, Cyber security mock drill, bug bounty, Red team versus blue team.



How the Problem solves: Primary objectives are identified plan in cyber security:

- Securing cyber space and Security R&D.
- Preventing cyber-attacks with study of current attacking trends and methodology.
- Reducing national vulnerability to cyber-attacks.
- Minimizing damage and recovery time from cyber-attacks.
- Capacity building & Regular Vulnerability Assessment and Penetration Testing of IT systems.
- Security of Information Assets in the context of newer vulnerabilities.



The cyber security challenges/ Issues to be addressed:

- Developing Effective security Policy, Legal framework, Compliance and Assurance.
- Security Incident: Early Warning and Response.
- National Cyber Alert System & Security R&D.
- How to report incident (CERT-In and Sectorial CERTs) information Exchange with other bodies.
- Domain Specific training: Cyber Forensics, Network & System Security Administration
- International & National Mock security drills.
- Skill & Competence development with Security training & Collaboration.

II. CONCLUSION

These are just a few of the conditions or scenarios you can use to test your incident response team's alertness or readiness for a cyber incident. Practicing these on a regular basis can help your security team be better prepared and identify any flaws before you are in the a crisis, saving you time, money, and peace of mind.

REFERENCES

[1] http://www.govtech.com/blogs/lohrmann-on-cybersecurity/A-new-cyber-exercise-Test-your-security-teams-incident-response-capabilities.html
[2] https://www.securitymetrics.com/blog/6-phases-incident-response-plan
[3] https://www.livemint.com/Politics/DGAZspP59udKsda4SsZy9M/Rise-in-cyber-crime-jolts-centre-into-action.html

