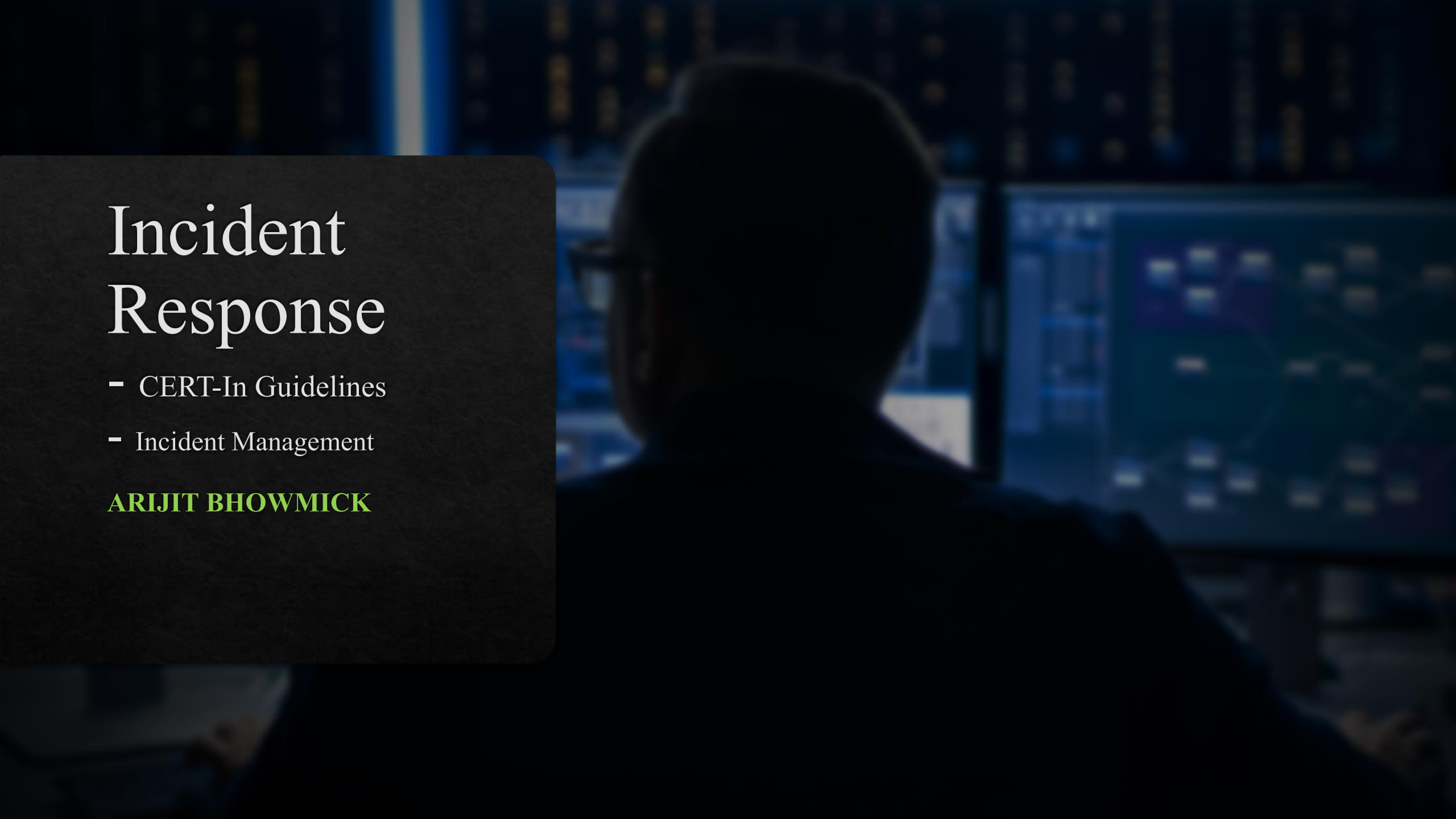

Incident Response

- CERT-In Guidelines
- Incident Management

ARIJIT BHOWMICK

Incident Response

- CERT-In Guidelines
- Incident Management

>> Customary Response Team Members

Info Technology		
CSIRT-IT	Sanitizing Team	Data Center
Security Operations Center	Server management	Mainframes
Information Security/Assurance Office	Database Administrator	Vulnerability Assessment
Help Desk	Web Developers	Classified Network
Forensics	Infrastructure Protection	Program Manager
Storage & Virtualization	COMSEC	Engineers
Malware Analysis	PKI Certificate Authority	Destruction
Penetration testers	Network & Sys Admin	End Users

Incident Response

- CERT-In Guidelines
- Incident Management

>> Understanding Role of Others in the Organization

- Different tasks in the Organization
- **CEO:** To maximize shareholder value
- **PR Officer:** To present a good image to the press
- **Corporate Risk:** To care about liabilities, good accounting, etc
- **CSIRT:** To prevent and resolve incidents

Incident Response

- CERT-In Guidelines
- Incident Management

>> Incident Response vs Incident Handling

• Incident Response is all of the technical components required in order to analyze and contain an incident.

Skills: requires strong networking, log analysis, and forensics skills.

• Incident Handling is the **logistics, communications, coordination, and planning functions** needed in order to resolve an incident in a calm efficient manner

Incident Response

- CERT-In Guidelines
- Incident Management

>> Dealing with Incidents – Bottom Line

- What happens if you don’t deal with incidents?

- Become Tomorrow’s headline (Image)
- Domain Blacklisted (Availability & Financial Loss)

- The World needs you!

- Trusted point of contact
- Doing your bit to keep the Internet a safe and secure place for everyone

Incident Response

- CERT-In Guidelines
- Incident Management

>> Incident Response

Incident response (IR) is the effort to quickly identify an attack, minimize its effects, contain damage, and remediate the cause to reduce the risk of future incidents.

Almost every company has, at some level, a process for incident response. However, for those companies looking to establish a more formal process, the pertinent questions one must ask are:

- What are the steps to activate the responsible parties involved in responding to an incident should one appear?
- How comprehensive and specific should your response plan be?
- Do you have enough people (and the right people) to respond appropriately?

What are your acceptable SLA's for responding to an incident and returning to normal operations?
Most likely, the answers to these questions will not be optimal, as most companies fall short in one area or more, according to a study by the Ponemon Institute:

- 77% of companies do not have a formal, consistently applied plan in place
- 57% indicate there has been an increased amount of time to respond
- 77% say they have a difficult time hiring and retaining security staff

Incident Response

- CERT-In Guidelines
- Incident Management

>> Phases of the Incident Response Lifecycle

There are six steps to incident response. These six steps occur in a cycle each time an incident occurs. The steps are:

- ✓ Preparation of systems and procedures
- ✓ Identification of incidents
- ✓ Containment of attackers and incident activity
- ✓ Eradication of attackers and re-entry options
- ✓ Recovery from incidents, including restoration of systems
- ✓ Lessons learned and application of feedback to the next round of preparation

Incident Response

- CERT-In Guidelines
- Incident Management

>> The ABCs of Incident Response

A.The Right Team

To deliver the most effective incident response, industry experts suggest including the following roles on your team, no matter the size of your company. Obviously, the technical team will take the lead, but there are other functional areas in your company that should be on board, especially if a severe attack occurs. Once the people for these roles are identified, educate them on what their responsibility would be in the event of a serious, extensive attack that has widespread ramifications: Incident response, Security analysis, IT, Threat research, Legal, Human resources, Corporate communications, Risk management, Executive, and External security forensic experts.

Incident Response

- CERT-In Guidelines
- Incident Management

>> The ABCs of Incident Response

B. The Right Plan

A comprehensive incident response plan includes the following tactics and processes at a minimum:

- Prepare and ready the team to handle any kind of threat
- Detect and identify the type and severity of an incident once it has occurred
- Contain and limit the damage
- Determine its impact and associated risks
- Find and eradicate the root cause
- Mitigate and resolve the attack
- Analyze and modify the plan post-attack to prevent future ones

Communication is key when an attack is underway, so ensure that you establish a good communication flow as part of your response plan.

Incident Response

- CERT-In Guidelines
- Incident Management

>> The ABCs of Incident Response

C. The Right Tools

With an increasing number of unknown attacks, the right tools may be able to save your company a lot of time and money – and it will help protect your customers and your brand loyalty.

Information is a critical asset for any incident response plan. Because of that, a cloud-based endpoint security solution typically provides you with the most comprehensive tools for mitigating attacks in the quickest manner, including access to key data through:

- Unfiltered data capture provides response teams with insights into endpoint behavior, not just previously discovered attack patterns and behaviors. This is the key to shorten an attack investigation from days to minutes, especially given the growing amount of unknown attack methods being leveraged today.
- Data analytics provide visibility into all endpoint activity, both present as well as historic. With the right data, you can see where the attack started and identify the path it took, all of which will help remediate it more quickly.
- External threat intelligence helps rapidly identify threats you haven't seen yet, but other companies have. Once again, if you know what you dealing with, you can respond more quickly.
- Live response capabilities help you remediate remote endpoints and eliminate unnecessary reimaging.

Incident Response

- CERT-In Guidelines
- Incident Management

>> Response Plan Components Review

- Identify Company Critical Assets
    - Who has them (system Owner)
    - Where they are located
    - Who has privileged access to them and what type
- What is Considered an Incident For You?
    - Human-Caused: Insider Threat, Untrained Staff
    - Natural-Caused: Tornadoes, Floods, Earthquakes
    - Technological-Caused: Power Grid Failure, Transportation Failure
- Require a Formal Incident Reporting System
- Determine a Category Escalation Matrix
- Incident Trigger-Employee, Self-report, Notice
- Roles and Responsibilities
- Investigation
- Communication and Information Sharing
- Cybersecurity information Sharing Act 2015
- Testing and Practice
- Maintenance and Updates of Response Plan

Incident Response

- CERT-In Guidelines
- Incident Management

>> What is CERT-IN ?

CERT-In (the Indian Computer Emergency Response Team) is a government-mandated information technology (IT) security organization. The purpose of CERT-In is to respond to computer security incidents, report on vulnerabilities and promote effective IT security practices throughout the country.

CERT-In was created by the Indian Department of Information Technology in 2004 and operates under the auspices of that department. According to the provisions of the Information Technology Amendment Act 2008, CERT-In is responsible for overseeing administration of the Act.

CERT organizations throughout the world are independent entities, although there may be coordinated activites among groups. The first CERT group was formed in the United States at Carnegie Mellon University.

Incident Response

- CERT-In Guidelines
- Incident Management

>> CERT-In - Its Role in Incident response

A CERT may focus on resolving incidents such as data breaches and denial-of-service attacks as well as providing alerts and incident handling guidelines. CERTs also conduct ongoing public awareness campaigns and engage in research aimed at improving security systems.

Regardless of whether they are called a CERT, CSIRT, IRT or any other similar name, the role of all computer emergency response teams is fairly comparable. All of these organizations are trying to accomplish the same incident response related goals of responding to computer security incidents to regain control and minimize damage, providing or assisting with effective incident response and recovery and preventing computer security incidents from reoccurring.

In general, an incident response team is responsible for protecting the organization from computer, network or cybersecurity problems that threaten an organization and its information. A universal model for incident response that has been in use for a long time is the “protect, detect and respond” model

CERT-In works towards the goal of enhancing cyber security in India. With this goal, this organization has defined its objectives as follows:

Prevention of cyber attacks that target the country’s cyber space
Responding to cyber attacks to minimize damage and reducing recovery time to ultimately minimize the national vulnerability to cyber attacks
Enhancing the level of cyber awareness among citizens

Incident Response

- CERT-In Guidelines
- Incident Management

>> CERT-In – Types of Incidents dealt

CERT-In addresses all cyber security incidents which occur in the country with a swift response to cut down further damage or loss of information. The cyber security incidents covered by CERT-In include:

- Physical cyber security threats to human beings.
- Severe cyber security incidents on any public information framework including backbone network infrastructure.
- Large-scale attacks like identity theft, intrusion into computer resources, website defacement, etc.
- Compromised user account on multi-user system.

Other than the above mentioned incidents, all the other incidents are prioritized according to their severity and extent.

Incident Response

- CERT-In Guidelines
- Incident Management

>> CERT-In - Functions

The functions of CERT-In have been assigned by the Information Technology (Amendment) Act 2008:

- CERT-In collects, analyzes, and shares information on cyber incidents taking place in India.
- Forecasts and alerts about cyber incidents.
- Takes emergency measures to handle cyber security incidents.
- Plays a major role in the coordination of cyber incident response activities.
- Issues guidelines and advisories in relation to information security best practices and procedures, prevention, and reporting of cyber incidents.
- Any other functions that relate to cyber security as prescribed.

Incident Response

- CERT-In Guidelines
- Incident Management

>> CERT-In - Empanelled Auditors

CERT-In has created a panel of IT Security Auditing Organizations that perform the vulnerability assessment and penetration testing of computer systems, networks & applications of various organizations that fall under the scope of the Government of India and those in other sectors of the Indian economy.

As per CERT-In, as a part of an audit, the empanelled security auditors may interview key people in-charge, carry out vulnerability assessments & penetration testing, list the existing security policies and controls, and test IT assets. This is carried out in order to determine the effectiveness of information security controls.

In this pursuit, the empanelled security auditor organization performs the following functions:

- IT security policy review
- Information Security Testing
- Internet Technology Security Testing
- Process Security Testing
- Application security testing
- Communications Security Testing
- Wireless Security Testing
- Physical Security Testing

Incident Response

- CERT-In Guidelines
- Incident Management

>> Guidelines on Incident management by CERT-In

Types of cyber security incidents mandatorily to be reported by service providers, intermediaries, data centres, body corporate and Government organizations to CERT-In:

- Targeted scanning/probing of critical networks/systems
- Compromise of critical systems/information
- Unauthorized access of IT systems/data
- Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites etc.
- Malicious code attacks such as spreading of virus/worm/Trojan/Bots/ Spyware/Ransomware/Crypto miners
- Attack on servers such as Database, Mail and DNS and network devices such as Routers
- Identity Theft, spoofing and phishing attacks
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- Attacks on Critical infrastructure, SCADA and operational technology systems and Wireless networks
- Attacks on Application such as E-Governance, E-Commerce etc.
- Data Breach
- Data Leak
- Attacks on Internet of Things (IoT) devices and associated systems, networks, software, servers
- Attacks or incident affecting Digital Payment systems
- Attacks through Malicious mobile Apps
- Fake mobile Apps
- Unauthorised access to social media accounts Attacks or malicious/ suspicious activities affecting Cloud computing systems/servers/software/applications
- Attacks or malicious/suspicious activities affecting systems/ servers/ networks/ software/ applications related to Big Data, Block chain, virtual assets, virtual asset exchanges, custodian wallets, Robotics, 3D and 4D Printing, additive manufacturing, Drones
- Attacks or malicious/ suspicious activities affecting systems/ servers/software/ applications related to Artificial Intelligence and Machine Learning

THANK YOU