

## Cyber Incident Response Fast, Thorough, Decisive

- 70–90% of malware samples are unique to an organization
- In 60% of cases, attackers are able to compromise an organisation's security within minutes
- 50% of employees open emails and click on phishing links within the first hour of receiving them

Source: <https://msisac.cisecurity.org/whitepaper/documents/1.pdf>

Cyberattacks can result in loss of data, finances and reputation, along with IP theft and operational disruptions. Additionally, they have legal implications.

### MODUS OPERANDI OF CYBERATTACKS

#### THREAT ACTORS - THE PEOPLE INVOLVED



- Non-state actors
- Organised crime syndicates
- Ideological groups
- Individuals

#### ACTOR ECOSYSTEM - WHO SUPPORTS THEM



- Malware authors
- Hosting entities
- Payment processors
- Domain generators
- Command and control
- Money mules

#### TOOLS, TACTICS AND PROCEDURES



- Social engineering
- Botnets
- Phishing
- Ransomware and doxing
- Exploits
- Website compromise
- DDoS Password theft
- Evasion tactics

#### THREAT VECTOR - THE CHANNELS USED



- Suppliers and partners
- Employees
- Mobile devices
- Smart devices
- Customers
- Email

### KEY ORGANIZATIONAL CHALLENGES

#### IT COMPLEXITY

- Endpoint diversity, with evolved IT structures supporting aspects like Bring Your Own Device (BYOD)
- Unauthorised devices connected to the organisation network
- Hosting new IT initiatives around cloud computing
- Demand for innovative IT solutions and real-time access to information across various devices
- Access provided to third-party entities

#### OPERATIONAL CHALLENGES

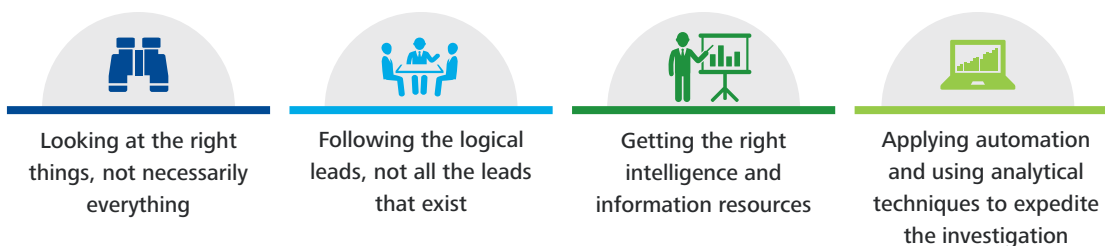
- Reliance on signature-based controls
- Limited data encryption
- Reliance on device-focused monitoring
- Insufficient skills/staffing in the IT security area

#### PROCESS/GOVERNANCE CONSTRAINTS

- Limited change control process
- Lack of business risk alignment
- Limited security of the Software Development Life Cycle (SDLC)
- Improper business risk alignment
- Limited extent of asset mapping to risks
- Inadequate/irregular training and awareness for employees

**AS ORGANISATIONS WITNESS RISING CYBERATTACK INCIDENTS, ONE OF THE KEY ASPECTS TO CONSIDER IS INCIDENT RESPONSE AND CONTAINMENT.**

An effective incident response begins with intelligent investigation



**HOW CAN DELOITTE HELP ORGANISATIONS WITH INCIDENT RESPONSE AND CONTAINMENT?**

Conduct a comprehensive investigation	Assess damages	Assist with response plan
<p>This is done to:</p> <ul style="list-style-type: none"> <li>• Understand the potential scale of the incident</li> <li>• Detect the locations of potentially compromised systems</li> <li>• Identify, preserve and examine logs available for the incident</li> <li>• Determine any priority systems or logs with a tier-based system for further collection and examination</li> <li>• Identify if an immediate, remote assessment or collection is required</li> </ul>	<p>Assessing the damage caused is vital to ascertaining the data accessed or exposed. It also provides an understanding of the information that the perpetrator might have sought for. We assess the damages by looking at the:</p> <ul style="list-style-type: none"> <li>• Files accessed</li> <li>• Indicators of file use and adversary intelligence gathering</li> <li>• Files potentially or actually breached</li> <li>• Hacker’s immediate steps after the attack</li> </ul>	<p>Our cyber forensic specialists can assist you with a cyber incident response plan that addresses:</p> <ul style="list-style-type: none"> <li>• Responsibility matrix in the event of an incident</li> <li>• Root cause analysis and right diagnosis (situational analysis of the potential impact such as impacted parties, information involved, etc.)</li> <li>• Remediation plan</li> </ul>

Please reach out to:

**Rohit Mahajan**  
 APAC Leader & Head - Forensic  
 Financial Advisory  
 Tel: +91 22 6185 5180  
 Email: rmahajan@deloitte.com

**Jayant Saran**  
 Partner  
 Forensic Financial Advisory  
 Tel: +91 124 679 3607  
 Email: jsaran@deloitte.com

**Jimmy Mate**  
 Senior Manager  
 Forensic - Financial Advisory  
 Tel: +91 20 6624 4610  
 Email: jmate@deloitte.com

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms. This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP).

This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.

©2016 Deloitte Touche Tohmatsu India LLP. Member of Deloitte Touche Tohmatsu Limited

Deloitte Touche Tohmatsu India Private Limited (U74140MH199 5PTC093339), a private company limited by shares, was converted into Deloitte Touche Tohmatsu India LLP, a limited liability partnership (LLP Identification No. AAE-8458) with effect from October 1, 2015