Cybersecurity Incident Response Plan for Tata Consultancy Services (TCS)

Name: Yash Sanjaybhai Patel

Student ID: 134094184

Course: CYT145 - IT Security: Ethical and Legal Issues

Professor: Ionut Anghelache

Date: October 23, 2025

➢ How and When to Use the Incident Response Plan

This Incident Response Plan explains how TCS should act when a cybersecurity problem occurs. The main goal is to control the situation quickly, reduce the impact, and restore regular business operations as soon as possible. TCS works with many clients worldwide, and even a minor security incident can impact a large number of users and affect the company's reputation.

This plan should take effect immediately when there are signs of suspicious activities like unusual network traffic, unknown login, or any missing files. For example, if any employee receives a fake email asking for important information, or if unusual traffic is detected on the company server, the security team should follow this plan.

This plan is also helpful during regular security testing and training sessions for the employees. Practicing this plan ensures that all staff know their roles, responsibilities, and how to respond during a real attack.

➢ **Event Handling**

Event handling is the process of identifying, reporting, and managing cybersecurity events in a planned way. At TCS, different types of security events can happen each day, so proper classification and action steps are critical.

Common types of events can include phishing, malware infections, unauthorized access, data leaks, and Denial of Service (DoS) attacks. For example, phishing occurs when an attacker sends fake emails to employees, pretending to be legitimate, and then requests their login information. Malware or ransomware infection occurs when harmful software is installed on a user's machine through downloads or email attachments that lock essential files. Unauthorized access occurs when someone outside the company logs into internal systems without permission, while a DoS attack floods the company's servers, preventing users from accessing websites or portals.

When an event occurs, the response should follow the steps below:

1. Detection: Using security tools such as firewalls and monitoring systems to identify suspicious activities.
2. Verification: Confirming that the alert is real and not a false alarm.
3. Classification: Deciding whether the issue is low, medium, or high risk.
4. Containment: Isolate the affected systems to stop the attack from spreading.
5. Investigation: Find the logs and systems to see how the attack was done.
6. Eradication: Removing malware, blocking suspicious IP addresses, and closing security gaps.
7. Recovery: Restoring the systems from safe backups and testing them before going online.
8. Documentation: Recording and documenting what happened, who handled the situation, and what actions were taken.

All incidents should be logged with date, time, and the team that handled the situation. Employees should also report suspicious emails or activities to the IT team immediately. TCS should also conduct sessions to keep everyone updated about the latest threats and how to prevent them.

At TCS, the classification of an issue determines the speed and type of response. A high-risk event, such as a ransomware attack on a server, receives immediate attention from senior engineers and legal advisors. Lower risk events, such as login failures, are logged and monitored before further action is taken.

All Employees should be trained to use the internal incident reporting tool to report suspicious activity directly to the cybersecurity team. This tool can help TCS respond more quickly and track threats.

➢ **Incident Response Team**

TCS has a professional Incident Response Team (IRT) that works together whenever a security event occurs. The team includes members from different departments, enabling both technical and business actions to be taken as soon as possible.

The Incident Response Manager leads the team, coordinates all the actions, and reports to senior management. The security Analyst investigates alerts, collects data, and monitors systems for threats. The Network Engineer handles routers, firewalls, and network traffic control. The Cloud Security Engineer manages security for cloud systems such as AWS or Azure. The Legal Advisor ensures that all actions comply with data protection and privacy laws. The HR Representative supports internal communications with employees, and the Public Relations Officer handles external communication with media and clients. The System Administrator restores systems from backups and applies security patches.

The team conducts regular drills to ensure we are ready. Communication charts list the contact order so that everyone knows who to inform first. Backup members are also assigned in case the main point of contact from the staff is unavailable. This teamwork ensures a quick, organized, and lawful response to any cybersecurity issue.

In addition to these roles, the Incident Response Team should include a Security Awareness Trainer who will provide employees with education on reporting phishing, password management, and handling data safely. Basically, this will help reduce the number of incidents caused by human error. During the incident, the team communicates through secure channels such as Microsoft Teams or any management tool like ServiceNow.

➢ Response Plan

The response plan shows the actions to be taken for each type of cyber incident. It helps protect the company data and reduce business impact. TCS follows a structured process for responding to cyber incidents. The response depends on the type of threat, the affected information assets, and the potential business impact. Each scenario below shows how the company should react to minimizing data loss and service interruption.

Phishing or Email Attacks:

When a phishing email is found, employees must report it to the IT department right away. The IT team will block the sender, scan systems for malicious links, and ask users to change passwords immediately. If anyone clicks a fake link in an email, their computer will be checked for malware. The security team then sends a notice to all employees, cautioning them to be careful with similar messages.

Malware or Ransomware:

If malware or ransomware infects any system, the first step is to disconnect that computer from the network. The team uses antivirus and endpoint protection tools to remove the threat. Ransom should never be paid, as backups can restore lost data. After the cleanup, the system is patched and analyzed to determine how the attack was carried out, such as via a USB drive or an email attachment. During Malware incidents, the communications team should update clients whose data may be delayed and ensure that no sensitive details are leaked to the public before receiving official confirmation.

Unauthorized Access:

When unauthorized access is detected, the affected account is immediately locked, and its password is reset. Multi-Factor Authentication (MFA) is turned on for all related systems. Logs should be checked to see what the attacker viewed or changed. The legal and management teams should be informed if personal or client data was accessed.

Data Breach:

In the event of a data breach, all transfers from the affected servers should be halted. The privacy and legal teams check compliance with Canadian and international laws. Affected clients and employees are informed right away. After the breach, vulnerabilities are fixed, and the system is tested before returning to service.

Denial of Service (DoS) Attack:

During a DoS attack, the network engineer blocks suspicious IP addresses and works with the internet provider to implement additional filtering. Load balancers and cloud services help manage heavy traffic until the attack ends. Once operations are normal, system settings are reviewed and improved.

Insider Threats:

Sometimes problems arise within the company, such as an employee misusing their access. The Incident Response Team monitors activity logs and investigates unusual activities. Access rights are suspended for anyone involved, and HR handles disciplinary action.

Sometimes attackers don't steal data, but they change it. This can happen in financial reports or software code. In such cases, the IT team must compare backup versions, validate checksums, and confirm data integrity before systems go live again.

In any response, clear communication and coordination are essential. The Incident Response Manager needs to provide regular updates to the management on the progress, containment results, and recovery status. The IT and security team must keep detailed information and not forget to document the action taken, like which systems were disconnected, which accounts were reset, and what tools were used, which can be helpful during post-incident reviews and audits.

After every incident, the team conducts a post-incident analysis to identify lessons learned, implement improvements, and update documentation. This review is essential because it ensures the following response will be even faster and more effective.

Impact on the Organization

A cybersecurity attack could harm TCS in several ways. The most direct and significant effects can include financial losses from system repairs, legal costs, or client compensation. Operational downtime also causes delays in projects with clients, especially when clients' servers are affected.

Another serious problem could be reputation damage. TCS handles highly sensitive data for global clients, and if this is broken even for once, it can take years to rebuild. Competitors might use the incident to gain and attract clients, and new customers may hesitate to work with TCS in the future. Such breaches often become public through the news and social media, which can quickly spread negative attention.

There can also be legal and regulatory consequences if TCS fails to protect data in accordance with privacy laws such as the Canadian Privacy Act, GDPR, or other international data protection standards. Regulators may impose heavy fines and client lawsuits for loss of their data.

Cyberattacks can also affect employee morale and productivity. Staff may lose confidence in the company’s systems or become extra cautious, slowing down their work. A large-scale attack may also result in intellectual property loss, with the project's source code for confidential business strategies stolen. This could reduce the company’s project cancellations or delays.

For example, if a ransomware attack disrupts a financial project or delays software delivery, customer transactions and timelines may be affected. However, having a strong, regularly tested Incident Response Plan allows TCS to react quickly, reduce financial and legal risks, and recover faster from any disruption. It also helps maintain client confidence, proving that the company can handle a crisis effectively and continue providing secure, reliable services.

➢ **Conclusion**

By preparing this Incident Response Plan, I have gained insight into how big organizations like TCS manage cyber threats. I learned that planning and teamwork are more effective than reacting after an attack. A clear plan keeps employees aware of what to do, ensuring fast communication, and reduces mistakes during an attack.

The TCS approach focuses on early detection, quick containment, and complete recovery. Regular testing, training, and continuous improvement keep the company ready for future challenges. The key takeaway is that being prepared before an incident saves time, money, and trust afterwards.

➢ **Information Sources**

NIST, "NIST Computer Security Resource Center | CSRC," *Nist.gov*, 2019. https://csrc.nist.gov/

Tata Consultancy Services, "Tata Consultancy Services | Technology, Digital Solutions, Consulting," *Tcs.com*, 2025. https://www.tcs.com/

C. C. for C. Security, "Canadian Centre for Cyber Security," *Canadian Centre for Cyber Security*, Aug. 15, 2018. https://www.cyber.gc.ca/

"Upgrade Your Cybersecurity Incident Response Plan With a 7-Step Checklist," *PhoenixNAP Global IT Services*, 2019. https://phoenixnap.com/blog/cyber-security-incident-response-plan

"Microsoft Security Blog - Digital Security Tips and Solutions," *Microsoft Security Blog*. https://www.microsoft.com/security/blog