Esri UK and Esri Ireland IT Security Incident Response Plan

Purpose

The Security Incident Response Plan (SIRP) is designed to minimize the impact from a security incident through a well understood, streamlined, and repeatable approach coupled with continuous improvement in our detection and protection capabilities.

What is an IT Security Incident ?

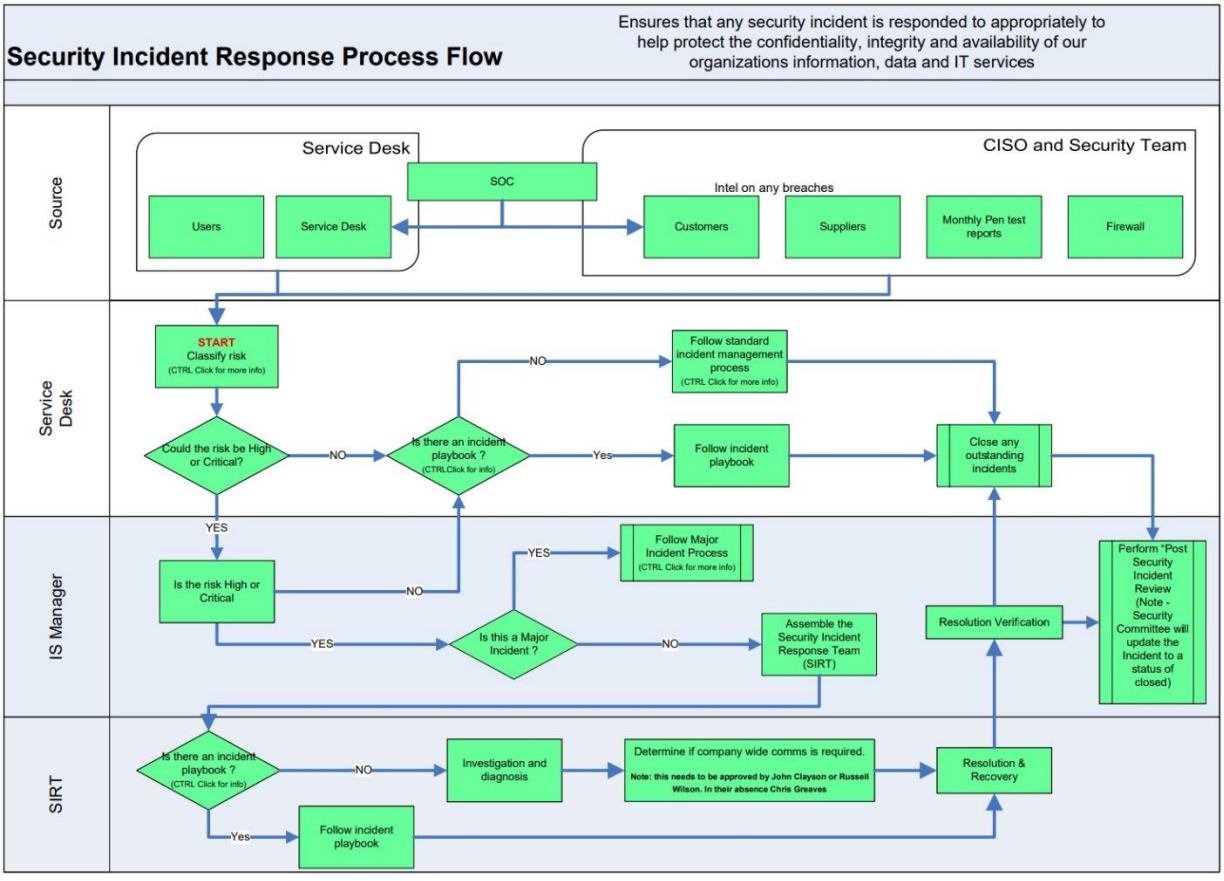
The SIRP will be triggered when a device is shown to be compromised in a manner that could result in the loss of data, service disruption, or lead to the compromise of additional systems. In addition, a security incident may also be an event which violates a relevant policy (for example, Computer Use Policy or Mobile Phone Policy) or standard security practice. Examples of a security incident could include Denial of Service, inappropriate device usage, malware, ransomware, or unauthorised access.

Preparation

Employees are trained to identify and report any suspected security incident to the Service Desk. Service Desk staff, and the wider IT team, are trained regularly on the incident response plan.

Incident Handling Process

Overview



Incident Detection

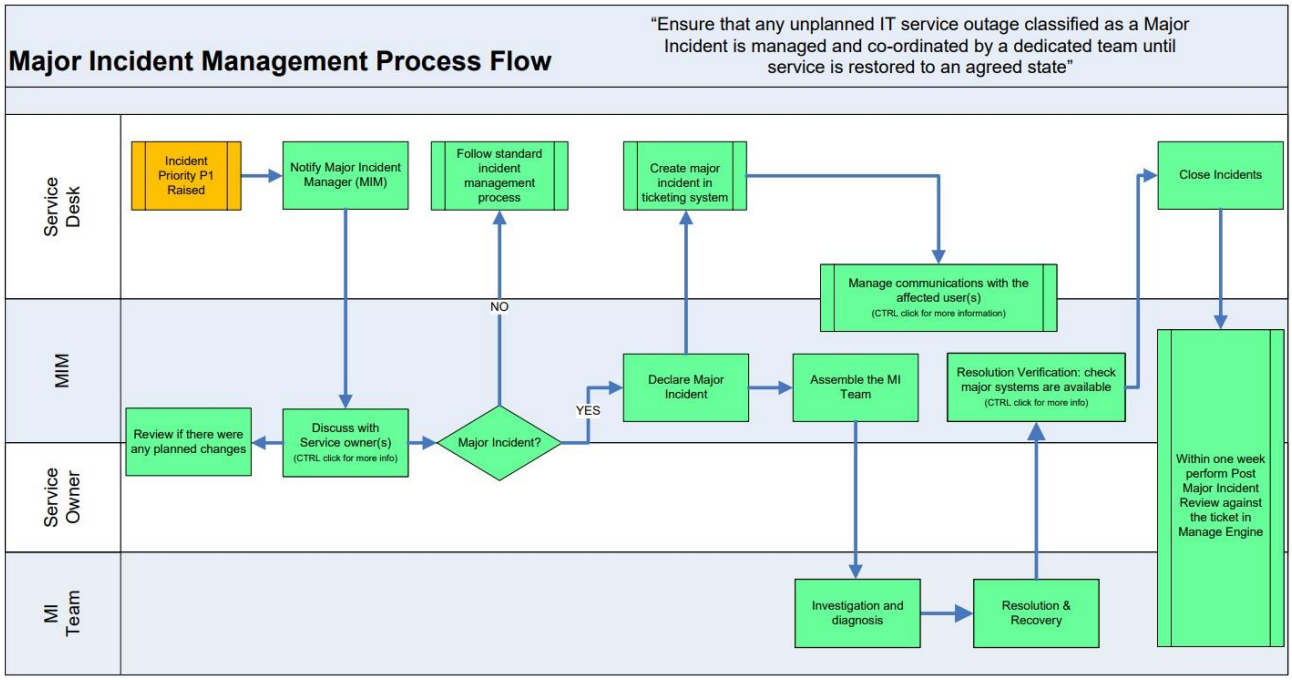
There are many channels through which a security incident can be detected:

- Security Operations Centre (SOC): Our main channel is through our 24/7 managed service SOC. The SOC ingests feeds from all laptops and critical (cloud hosted) servers, and alerts are triaged, analysed, and fed back to Esri UK when action is required.
- Firewall: Our 24/7 managed firewall provider informs us of any alerts requiring our attention
- Customers and Suppliers: Our customers and suppliers will provide warnings of compromised systems where they interact with our staff or our systems
- Service Desk: Users can report incidents via the Service Desk, and common alerts (such as AV alerts) are also automatically logged as tickets.
- Other Feeds: Information is reviewed regularly from sources such as NCSC, CISP and well-respected security news sources as well as through our outsourced cyber security 'retainer' contract.

Classification

All potential security incidents, reported directly via the Service Desk or through other feeds/sources are assessed to classify their risk. The initial classification, using a standard matrix, will consider if the risk is critical/significant or not.

- **Low/Medium:**
  For low/medium risks our standard incident management process is followed and supplemented by specific playbooks. Incidents are monitored to ensure that the risk does not become significant over time.
- **High/Critical:**
  If the incident is classified as high or critical an assessment is made on whether this constitutes a major incident. If it does, then the major incident process is followed (see next page for overview). If it is not a major incident then the Security Incident Response Team (SIRT) is convened and appropriate investigation, diagnosis and communication is undertaken, leading to resolution and recovery and a post incident review follow-up.



Security Incident Response Team (SIRT)

Esri UK and Esri Ireland's SIRT team consists of IT staff able to handle the response to IT security incidents. The personnel on the team will change dependant on the nature and extent of the incident, however, the core team will usually consist of IS Staff, IS Cyber Security Staff and the CISO or the CIO. The team will call upon other expertise across the business as required, this can include HR, Senior Management, members of the Cyber Security Authority and other subject matter experts. The team can also engage with our external partner as part of our security incident response retainer.

Communication

Internal

Internal communication will be coordinated by the SIRT or Major Incident Management (MIM) team. Communication will be via service desk ticket responses, email, portal posts or text messages depending on the scale and severity of the incident.

External

- Low/Medium: These will typically not require any external communication to a wider audience.
- High/Critical: These are not likely to require external communication, but if needed, should be coordinated via the CIO or CISO, Head of Legal, and Head of Marketing
- Major Incident: These are more likely to require external communication. The assigned communications lead for the incident will liaise with CIO or CISO, Head of Legal, and Head of Marketing before any communication is sent

Escalation

The SIRT or MIM Team may need to escalate an incident to senior managers and to our external security incident response partner. The following table provides examples to help guide staff on when escalation may be needed.

Impact	Escalation to
Low	CISO (Service Desk Team Lead if CISO is not available)
Medium	CISO > CIO
High	CIO > CTO and MD

Containment, Remediation and Recovery

All those involved in the incident will work to contain the incident, remediate it and where required, recover from it. All appropriate systems will be checked. This may include the invocation of our Disaster Recovery process.

Closure

Once any critical or serious incident has been resolved, there will be a review process undertaken by the SIRT or MIM Team to understand the lessons learnt, and any improvements or mitigations that will help prevent similar incidents occurring in the future. Any actions will be logged in our security improvements backlog and assessed and prioritised against other security improvements.