UNCC’s 11th Annual Cyber Security Symposium

Building a Computer Security Incident Response Team
An Enterprise Approach
Computer Security Incident Response Team

The Evolving Necessity
A Computer Security Incident Response Team (CSIRT) is a service within an organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity.

New types of information security risks emerge frequently and while preventive measures can assist in reducing the number of related incidents, not all incidents can be avoided.

An incident response capability is necessary for rapidly responding to incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring appropriate computing services.
Traditionally, computer security incidents were thought of primarily as cases of the introduction of malware (virus, etc.) or of “hackers” trying to break into a network environment. While these definitely still occur, there are other events that must be considered.

- Loss of computing equipment – with sensitive information?
- Non-malicious policy violations – human resources issue?
- Malicious policy violations – legal issue?
- Data leakage – industrial espionage or organized crime?

Much more than operational efficiency is at risk today.
Many people consider the risks of computer security incidents to be the loss of operational efficiency and the efforts expended to restore that loss.

Today, there are new, and in many cases, more serious risks to be considered.

- Regulatory compliance (PCI, HIPAA, etc.)
- Organization’s reputation
- Customer and partner confidence
- Intellectual property
- Legal liability (HR, copyrighted material, punitive damages, etc.)
- Personal liability (board of directors, etc.)
The Evolving Necessity: Why You Need CSIRT
Computer Security Incident Response Team

Assembling the Team
Assembling the Team: Typical View

In most organizations, incident response is handled in one of two ways:

- As an ancillary responsibility for one or more individuals in information security or information technology
- As a single individual or small group of individuals handling all aspects of incident response

A more effective incident response team is one comprised of individuals from a number of operational groups and departments.
Core CSIRT Team: Core CSIRT team members act as incident coordinators who are ultimately responsible for the final resolution of all computer security related incidents.

Extended CSIRT Team: Extended CSIRT team members are individuals within various operational departments possessing specific skills to assist in case actions and/or having intimate departmental and institutional knowledge.

Individual CSIRT Contributors: Individual CSIRT contributors are assigned specific actions to complete based on their knowledge, skill sets, and responsibilities.
CSIRT should primarily be an investigatory entity, focusing on determining the root cause of an incident as well as providing assistance to other investigative teams. Typically responsibilities include:

- Investigating potential security breaches where computer(s) may have played a role
- Investigating suspicious activities both internal and external to the organization
- Assisting and consulting with other organizational response teams during large scale incidents and outages
- Providing computer forensic capabilities to support CSIRT investigations and other processes such as e-discovery and legal holds
- Recommending remedial actions as appropriate
As an investigatory entity, core CSIRT primarily focuses on determining the root cause of an incident. In order to delineate boundaries of responsibilities, core CSIRT should not be the source of:

- Employee intervention, however CSIRT collaborates with Human Resources, Legal, and other departments on security incidents that are personnel related

- Legal interpretation, however CSIRT collaborates with various departments providing additional insight into investigations

- Remedial actions, however, CSIRT recommends corrective strategies and actions

These should be handled by extended CSIRT members or their designees.
Assembling the Team: Extended CSIRT Responsibilities

Extended CSIRT members have fundamentally a dual role. They serve as the point of contact for and the liaison between their department and core CSIRT, accepting CSIRT action requests and distributing them to appropriate personnel (CSIRT Individual Contributors) within their department. They may also sometimes fulfill CSIRT action requests themselves. Specific extended CSIRT responsibilities include the following:

- Understanding the organization’s CSIRT process and ensuring this process is followed for incidents identified by their department
- Identifying personnel within their department with the appropriate skill set and expertise to fulfill CSIRT action requests
- Personally fulfilling CSIRT action requests when appropriate
- Ensuring that a backup extended CSIRT member is identified for their department, and that this individual is aware of the responsibilities
Acting as the communications liaison for their department in the event an incident must be escalated to their department.

Maintaining confidentiality of all incident/case data and communicating the confidentiality requirement to individual contributors within their department.

Serving as a consultant/advisor to core CSIRT members regarding alternate means of fulfilling CSIRT action requests and on courses of action for handling incident responses.
Assembling the Team: Required Commitments

There are a number of commitments necessary for the organization to make to facilitate the successful implementation of the extended CSIRT model.

- Executive level support is vital

- Primary and back-up extended CSIRT members by department should be available

- Extended CSIRT training – initial and on-going training should be provided

With these in place, an effective and efficient extended CSIRT model can easily be implemented.
Computer Security Incident Response Team

Building the Process
The major elements of a CSIRT process must be defined, with each of the elements having accompanying detailed procedures.
An incident’s priority can be determined by establishing the highest level of impact on the organization using an established matrix.

In this example, the incident reflects a “Medium” priority even though most impacts are considered “Low”.

<table>
<thead>
<tr>
<th>Category</th>
<th>LOW (SLA – 24 hrs)</th>
<th>MEDIUM (SLA – 8 hrs)</th>
<th>HIGH (SLA – Immediate)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td>Little to None</td>
<td>$100K to $250K</td>
<td>&gt; $250K</td>
</tr>
<tr>
<td>Reputation</td>
<td>Little to None</td>
<td>Localized</td>
<td>Widespread</td>
</tr>
<tr>
<td>Regulatory</td>
<td>Minor to No Infrngt</td>
<td>Significant Infrngt without PII or PCI Data Disclosure</td>
<td>Disclosure of PII or PCI Information, Requiring Either Internal or External Notification</td>
</tr>
<tr>
<td>Operational</td>
<td>Little to None</td>
<td>Localized and/or Moderate Impact</td>
<td>Widespread and/or Severe Impact</td>
</tr>
<tr>
<td>Legal</td>
<td>Little to None</td>
<td>Legal Action (civil and/or criminal) Unlikely</td>
<td>Legal Action (civil and/or criminal) Likely</td>
</tr>
<tr>
<td>Policy</td>
<td>Minor to No Infrngt</td>
<td>Inappropriate but Not Malicious</td>
<td>Suspected Malicious Intent</td>
</tr>
<tr>
<td>Application</td>
<td>N/A</td>
<td>N/A</td>
<td>PCI, PII Data Breach</td>
</tr>
</tbody>
</table>
Now a CSIRT process can effectively utilize a Reporting Escalation Matrix to ascertain which departments should receive immediate alerts about an incident.

<table>
<thead>
<tr>
<th></th>
<th>LOW (SLA – 24 hrs)</th>
<th>MEDIUM (SLA – 8 hrs)</th>
<th>HIGH (SLA – Immediate)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td>CSIRT</td>
<td>RMC</td>
<td>Legal and Finance</td>
</tr>
<tr>
<td>Reputation</td>
<td>CSIRT</td>
<td>RMC</td>
<td>Global Communications</td>
</tr>
<tr>
<td>Regulatory</td>
<td>CSIRT</td>
<td>RMC and Legal</td>
<td>Global Communications</td>
</tr>
<tr>
<td>Operational</td>
<td>CSIRT</td>
<td>Security Operations, GIS and RMC</td>
<td>GIS Major Incident</td>
</tr>
<tr>
<td>Legal</td>
<td>CSIRT and RMC</td>
<td>Legal</td>
<td>Legal</td>
</tr>
<tr>
<td>Policy</td>
<td>CSIRT</td>
<td>RMC and Human Resources</td>
<td>Legal</td>
</tr>
<tr>
<td>Applications</td>
<td>N/A</td>
<td>Affected Asset Owner(s)</td>
<td>Affected Asset Owner(s)</td>
</tr>
</tbody>
</table>
Once an incident has been properly categorized, utilizing a response matrix ensures that incidents are handled in a standard and repeatable fashion.
Building the Process: Continuous Improvement

A feedback process is important. This should be done by both CSIRT’s “clients” and internally by core CSIRT. Constructive feedback allows the process to be continually improved.
The result is a codified, documented process guide that serves multiple functions.

- Reference for both incident responders and various organizational departments
- Satisfy regulatory requirements
- Evidence documentation for internal and external audits
- Support for court cases
Thank You

Jim Bothe
jbothe@acmbs.com

Tony Poplin
tpoplin@acmbs.com