Computer Security Incident Response Team Charter

Purpose

This Charter defines the scope, goals, authority, membership, roles, and responsibilities for the Computer Security Incident Response Team (CSIRT).

Scope

The CSIRT will define, maintain, and execute the Computer Security Incident Response Plan (CSIRP). The CSIRP defines the policies, processes, methodologies, resources, roles, and responsibilities required to investigate and remedy any computer or network security events or incidents within the networks, as well as any networks or entities that interface with the network.

The CSIRT will execute the appropriate coordination required to apprise the applicable stakeholders, technical, managerial, and administrative decision makers of incident mitigation requirements in a timely manner. The CSIRT will provide governance and guidance, oversight of, and recommendations concerning, all aspects of the CSIRP. This includes best practices, investments, incident management systems, policies, procedures, definitions of roles and responsibilities, and coordination needed for the effective and efficient mitigation of computer security incidents that impact the organization. The CSIRT's immediate scope of responsibility and priority is to investigate computer or network security incidents relating to the following computing and communications infrastructure:

- Networks (including the network at core facilities, WAN connections)
- Remote Access Networks
- VPN Networks
- Any hosts that reside on the networks named above
- Any networks that interface with any of the networks

The CSIRT will also be responsible for assisting the following entities when network or computer security incidents reach beyond the scope identified above:

- All business partners connected to the network or using the Internet to communicate with this organization
- All governing state and federal agencies and organizations as related to this business

- All levels of law enforcement
- All associations and organizations related to the utilities industry, emergency or incident response roles, and security (CERT, FIRST, etc.)

Goals

The main goal of the CSIRT is responding to an investigation of security incidents. The CSIRT is also committed to the following additional goals:

- Providing feedback for the continued development of the business security architecture to reduce the likelihood of a security incident
- Maintaining appropriate hardware and software tools to facilitate proper investigations
- Keeping CSIRP members trained on current investigative and forensic techniques
- Communicating with all the appropriate parties on a timely basis
- Sharing pertinent information with all business partners and other appropriate parties to strengthen the overall security of the company
- Developing and maintaining open working relationships with all business units, departments and divisions, as well as with the board of directors
- Developing and maintaining open working relationships with the organization's internal audit group
- Developing and maintaining open working relationships with network support (routed networks), system administration (UNIX, desktop support), network management, and database administration personnel
- Developing liaisons with business partners' incident response team(s) (IRTs), network engineers, information security personnel, outsourced vendors, or other authorized personnel
- Developing a liaison with FIRST, HTCIA, and CERT

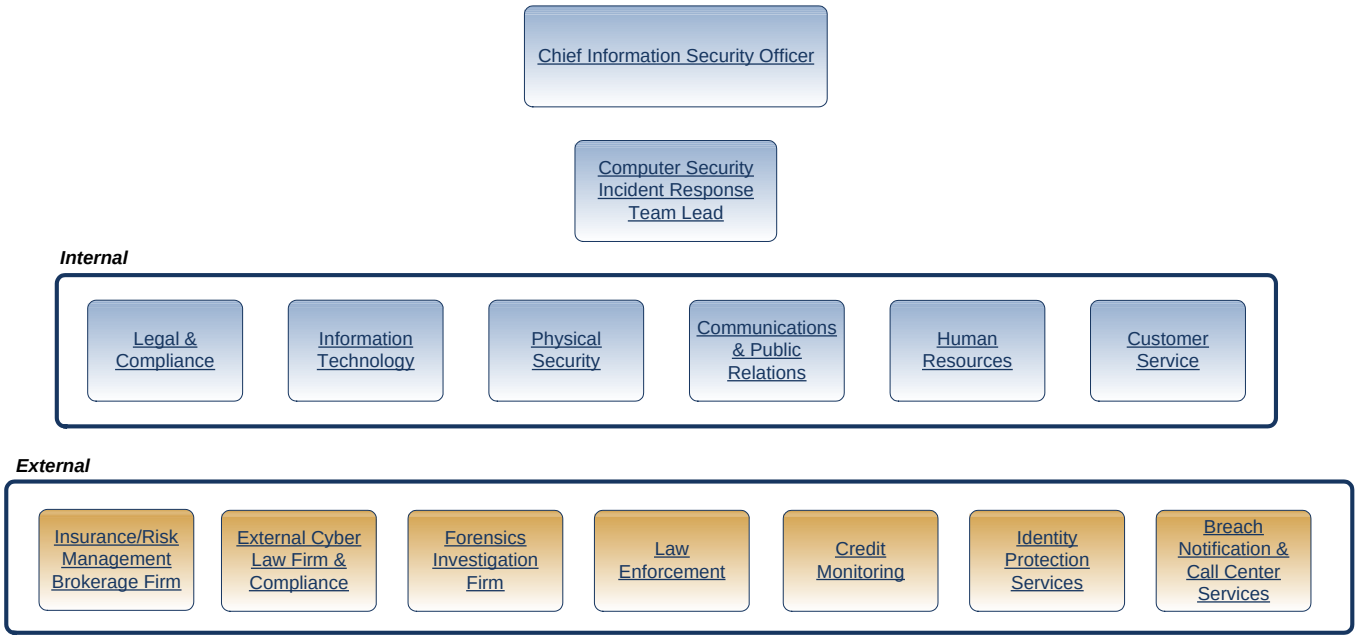
Authority

The Chief Information Officer (CIO) is the CSIRT sponsor. The Chief Information Security Officer (CISO) is the responsible leadership. The CSIRT has the authority to oversee and make recommendations regarding the incident mitigation domain. The CSIRT will execute its duties within the scope of this Charter, as informed by any applicable laws, regulations, directives, and any additional assignments of responsibility from external governance bodies.

Membership

Numerous teams are critical to the organization's security. Team membership is dictated by the efforts required to efficiently and effectively mitigate the effects of a cybersecurity incident. The following charts illustrate the internal and external general membership requirements encompassing foreseeable computer security incident response efforts. Configurations of membership activation depend upon the requirements defined by specific incident encounters.

Computer Security Incident Response Team (CSIRT)



CSIRT Internal Members' Roles and Responsibilities

The CSIRT is lead by the Chief Information Security Officer (CISO). The additional team component roles and responsibilities are as follows:

- Computer Security Incident Response Team Leader
  - One of the individuals listed as the Core Team Members will be assigned the role of Incident Response Lead for the Incident Response Team for each security incident. The Incident Response Lead is the leader of the Incident Response Team during the entire course of the security incident
- Information Technology
  - Lead the technology efforts
    - Suspicious event monitoring and detection

        - Incident analysis
        - Incident containment, eradication, and recovery
        - Post-Incident activities
    - Provide Incident Response Handlers and Forensics
- Legal & Compliance
    - Legal counsel - The information prepared during an attorney-led investigation may be protected by the attorney-client privilege or attorney work product doctrine in the event of litigation
    - Shape your data breach response and help minimize the risk of litigation and fines
    - Determine how to notify affected individuals, the media, law enforcement, government agencies and other third parties, such as card holder issuers, if needed
    - Establish relationships with any necessary external counsel before a breach occurs
    - Review and stay up to date on both state and federal laws governing data security
- Communications and Public Relations
    - Depending on the size of the data breach and industry, the organization may need to report the breach to the media and/or notify affected individuals
    - Identify the best notification and crisis management tactics before a breach ever occurs
    - Handle any information leaks regarding a breach
    - Track and analyze media coverage and quickly respond to any negative press during a breach.
- Human Resources
    - Human resources is responsible for managing the aspects of an incident as it affects the organization's employees
    - Maintain proactive and frequent communications with employees to the extent practical about the cyber incident
    - Preplan and test employee communication protocols
    - If employee sensitive data is involved, ensure adequate remedies are in place
- Customer Service
    - Customer service may be the most personal and frequent communication between the organization and the data breach victims. Customer service reflects the organization's commitment to customers and victims during an incident
    - Develop communications protocols
    - Ensure customer service representative are intimately familiar with the communications protocols
    - Invest in communications training for customer service representatives
    - Prepare customer service Q&As

- Create simulation training for your customer service representatives that demonstrates how their roles would change during a data breach
- Outline a plan for setting up a customer cyber incident hotline
- Plan for the use of external resources if applicable

CSIRT External Members' Roles and Responsibilities

In some circumstances, the Incident Response Team will need to request external resources for assistance. Usually, the use of external resources will not require disclosure of information related to the security incident. However, if divulging information related to the security incident is required, the legal team and appropriate compliance areas must be involved and must have executive management approval before the information is released to the external parties.

- Insurance/Risk Management Brokerage Firm
  - The cyber security liability insurance policy may stipulate that the insurance company be notified early in the incident management process and that the organization will use external services authorized by the insurance company. Refer to the Cyber Liability & Privacy Insurance Playbook.
  - Insurance/Risk Management Brokerage Firm may cover:
    - Forensic investigation and system restoration
    - Defense and indemnity costs associated with litigation resulting from the loss of personal information or other sensitive data
    - Defense costs and penalties associated with regulatory investigations
    - Notification costs and credit monitoring for affected customers and employees
    - Losses attributable to the theft of the policyholder-company's own data (including transfer of funds)
    - Business interruption costs attributable to a cyber attack
    - Costs required to investigate threats of cyber-extortion and payments to extortionists
    - Crisis management costs, such as the hiring of public relations firms
- Law Enforcement
  - Depending on the severity of a incident, law enforcement may need to be involved
  - Identify which law enforcement agencies including the FBI, Secret Service, State Attorney General, and local law enforcement to contact in the event of a data breach involving criminal activity
  - During an incident, ensure everyone on the response team is aware of any law enforcement directives so the investigation isn't interrupted

- Extended Response Team
  - Technical
  - Managerial and Administrative
    - Executive Management will support the CSIRT by ensuring the cooperation and support from all involved parties. They will ensure the CSIRT has access to all resources to conduct its functions, as well as assistance from all personnel until the CSIRP activities are completed.

EFFECTIVE DATE AND TERMINATION

This Charter shall be effective upon approval by the (appropriate authority) and signed by the (appropriate authority). This Charter will remain in effect until amended or replaced or until terminated by the (appropriate authority).

SIGNATORY APPROVAL

_____ _____

Chief Information Officer Date

_____ _____

Chief Information Security Officer Date