Portland Community College
Incident Response Plan - *Draft*
24 x 7 Operations

Table of Contents

Introduction

There are many elegant definitions of a security incident. In reality, a security event is any activity or suspicious event that is outside of normal information technology operating practices and parameters. All of these events should be reported and investigated by a qualified subject matter expert. A very high percentage of first detected anomalies will be false positives, user errors or technology problems. However, a few will be very real incidents incorporating the possibility of high risks to PCC or its students.

It would be nice to state that cyber security incidents always perform in a uniform and predictable manner, but they do not. Cyber incidents are capable of stealth like operations hiding from detection and changing as fast as the criminal elements can develop new technologies and delivery approaches. Security vendors like McAfee and Microsoft have to reverse engineer the technology created by the criminal in order to issue update patches and this takes time in the form of months and money, while the criminal element can change their attack code in hours with very little cost.

Today, the definition of an incident is expanding to encompass a broad spectrum of possibilities, activities and concerns. Many concerns are directly related to cyber security while others involve aspects of general Information Technology operations, regulatory compliance, telecommunications, support channels and physical security controls.

To meet the challenges of criminal activities today a well-trained cyber team is required to deal with the technology complexities while reducing the risk and preserving Portland Community College's vital assets. This is the role of the Incident Response Team.

Scope

Portland Community College Incident Response Plan (IRP) ***represents a change in current business practices*** by rating and defining the approved processes, procedures, and guidelines for an Incident Response Team (IRT) to follow. These processes and procedures are designed to mitigate risks, reduce costs and reduce down times due to a security incident or catastrophic anomaly.

This document does not contain technically detailed "how to" information, PCC engineers understand the complexity of their positions and the systems they are supporting. Instead, the plan provides a practical road map of what to do during such chaotic events.

Purpose

The purpose of this Incident Response Plan is to outline a set of response requirements that are pre-approved ensuring cyber security, PCC business, education, and regulatory compliance regulations are adhered to with the primary goals of protecting PCC's assets, people, students, and resuming normal operations as quickly as possible.

The primary benefit of having a well-developed incident response plan combined with a highly trained response team is operational symmetry by systematically following a pre-defined and consistent incident handling methodology.

Plan Guidance

Education, engineering, telecommunications, information technology and data transport systems combined with other critical data assets are making use of Internet connectivity and next generation technologies to boost productivity, improve efficiency and reduce operating costs. However, the Internet represents global connectivity which is an environment associated with both good and the high risks of cyber threats. Incident response planning prepares the organization for such emergencies by focusing the response team on pre-approved action plans that manage the risks of a breach, malware and other catastrophic failures systematically.

Incident Response Plan - IRP

Today, it is critical for an organization to have an effective incident response plan supporting both disasters and security incidents. These plans combined with a well-trained team are capable of recovering from an adverse event, resuming business operations and supporting regulatory or legal actions. This response plan develops, educates, trains, audits and relies on the team approach to support a series of common undertakings:

- Identifying security incidents
- Resolving an incident quickly
- Protecting assets and reducing losses
- Recovering from a security event
- Mitigating future organizational risks or exposures
- Reducing the chaos of crises
- Proper and consistent documentation

This plan will redefine several roles and responsibilities within PCC-TSS and the Incident Response Team. The help desk and its current extension x4400 will continue to be the central reporting authority for all PCC.

- IRM - Incident Response Manager - Val Moreno
- ISM – Information Security Manager – Terry Nickerson
- IRT - Incident Response Team
  - Team Lead
  - Operating system analyst
  - Networking analyst
  - Application analyst
  - Forensics analyst
  - Physical security

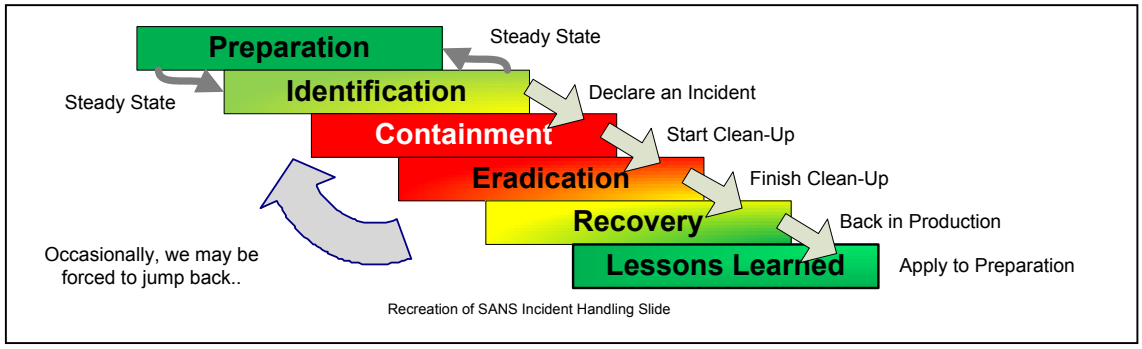
An Incident Response Plan (IRP) must encompass a wide arena of focus, for example a computer breach is legally one aspect, while a computer misuse event is a whole different spectrum of concern and response, while a disaster is yet another type of chaotic event and response altogether.

To be an effective tool the IRP must incorporate the many aspects of PCC's business and operations in managing incident response processes. The first aspects of the plan must have provisions to discover, identify and triage a true incident over a false positive event. In many cases this may be time critical as many cyber events are pervasive in their attack structure. Through common "Best Practices and NIST Guidance" the plan assigns each event a degree of urgency by priority ranking which defines an action plan associated with risk and initiates specific response teams, technologies and business groups.

Methodology

The methodology for this incident response plan reflects the current design and "Best Practices" of National Institute of Standards and Technology Publications NIST 800-53, NIST 800-61, NIST 800-83 and the SANS Institute.

The Incident Response Plan creates 6 individual operating elements, which have been defined by national regulatory groups, compliance laws and law enforcement.



For organizations the size of PCC a recommend seventh operating element called Case Management is recommended. This last element correlates all of the incident and forensic documentation into a single file combined with associated legal case information. Incident reports must define the incident in detailed terms. If the case is to be prosecuted a legal chain of evidence is required and the Incident Response Manger must understand these operational terms.

Preparation Phase

Preparation supports three goals:

1. First it is a quiescent starting point for each suspected incident or anomaly.
2. The second goal of preparation is to report an anomaly to the various teams that can handle a specific incident.
3. The third goal develops critical response resources to support the incident. Activating the IRM (manger) with the possibility of activating the IRT (team).

Requirements:

- Define "team" roles and responsibilities as it applies to each incident
- Procedures (e.g., system integrity checks, account expiration, patch application, investigation)
- Have the required security tools combined with use training

Identification Phase – SIEV Rating

The identification phase is ***often the most challenging process***. It involves, first, detecting an anomaly then determining whether the observed occurrences are a false positive event or an active risk or threat to PCC, and time can be a critical element.

Ranking an incident defines the severity of the event in terms of risk, loss, procedures and recovery.

Risks = Threats x Vulnerabilities x Impact
https://www.owasp.org/index.php/Threat_Risk_Modeling

Threat Modeling and Identification System - SIV

There are a variety of ways that TSS staff could become aware of the malicious infiltration, such as a user calling the Help Desk with a frozen workstation, a Systems Analyst noticing that an application is malfunctioning with no legitimate cause, or a public entity notifying the Manager of Information Security that there is an issue. The TSS staff member that becomes aware of a potential Security Incident should use the following rating scale to determine the Priority. The Priority will dictate the level of response, such as whether TSS staff is expected to drop all other work to respond to the incident.

The Priority Score will be used to determine the incident's importance relative to other work being performed by TSS and other issues being addressed by the College. The score will be

calculated by the TSS staff that initially becomes aware of the incident, and it will be updated by the Incident Manager or the Manager of Information Security as more information becomes available. The score consists of three factors, in the format S-I-E-V, which will be calculated as follows:

S- Sensitivity is the degree to which there is evidence that sensitive data, including Payment Card Industry (PCI), Personal Health Information (PHI), Personally Identifiable Information (PII), is being maliciously accessed:

0 - No evidence of sensitive data involved
1 - Minor evidence of sensitive data being accessed (e.g., a high value workstation has a ghost attack)
2 - Moderate
3 - High (e.g., malware found on a workstation or server that handles sensitive data)
4 - Very High to be used when there is solid evidence that sensitive data is being sent externally (e.g., man in the middle attack on a workstation or server that handles sensitive data)

I - Inoperability is the degree to which the College's systems are not functioning due to a security incident:

0 - No sign of any systems being negatively impacted operationally
1 - Minor system malfunction (e.g., no more than five workstations not functioning)
2 - Moderate
3 - High (e.g., malfunction of an application used by more than 10 people)
4 - Very High (e.g., malfunction of an application used by more than 1000 people)

E - Economic impact is a measure of the risk of a direct cost imposed by a third party as a result of the incident. It is a measure of the probability that a third party, such as the federal government, will impose a penalty on the College or the likelihood that other fees, such as legal fees, will be incurred. The rating will reflect the likelihood of the direct economic impact as well as the dollar amount. This category does not include *indirect* economic impacts, such as student enrollment declining due to lack of trust or increased administrative costs due to systems not working as designed (these impacts are captured in the "V" and "I" ratings, respectively)

0 - No likelihood of a direct economic impact

1 - Minor fees or fines may be incurred but will be less than $5000

2 - Moderate fees or fines could be incurred up to $50,000

3 - High fees or fines could be incurred up to $100,000

4 - Very High fees or fines could be incurred over $100,000

V - Visibility is the degree to which the security incident is or could be known externally to PCC and cause damage to PCC's reputation:

0 - no threat of external disclosure
1 - Minor
2- Moderate

3 - High (e.g., PCC website displays a compromise, PCC systems attacking external targets)
4 - Very High (e.g., incident must be disclosed publicly due to regulations)

If at least one of the four factors has a score of 3 or above, the incident will immediately be brought to the attention of TSS Management, who will set appropriate priorities to ensure that the incident is being responded to appropriately.

Containment Phase

When an incident has been detected and analyzed, it is important and often critical to contain and or isolate the incident as soon as possible before more information or assets are lost, or the anomaly spreads overwhelming resources. Time is often critical! However, forensic information must be preserved and the call for containment must be made by a subject matter expert within the incident responses team.

Typical containment decisions might be:

- Shut down a system or multiple systems – *risk losing forensic data / significant down time for business operations*
- Shut down a complete network segment – *risk losing forensic data / significant down time for business operations*
- Re-boot the system or systems – *risk losing forensic data*
- Disconnect the systems from a wired or wireless network
- Disable certain functions
- Firewall changes to isolate the impacted area

Containment strategies vary based on the type of incident and the risks involved. For example, the overall strategy for containing an email-borne virus infection is quite different from that of a network-based Trojan-Horse infection or a direct intrusion. Therefore separate containment strategies have to be tailored for each specific incident.

Containment or isolation strategies can be complex, while powering the system off or disconnecting the network cable seems to be a simplistic form of containment, in many cases it is not the correct decision. For a single server event, simply disconnecting the network cable might make sense. It preserves the information and limits the spread of the problem through isolation. However, this can be a catastrophic answer to a production server like Banner which might affect business and operations on other servers. The alternative might be to let the problem continue while working on a solution. The simple facts are mission critical systems and certain applications simply cannot be down. These systems require a more complex containment strategy combined with a strong forensics approach that only subject matter experts can make.

Containment and mitigation in both the short term and the long term are key factors in further eradication and mitigation strategies. Long-term containment strategies entail a current forensic investigation, understanding the incident's make-up and design and a strategy for resuming business operations safely, combined with a full review of back up and data storage reservoirs to understand if the anomaly migrated to storage.

Requirements

- Notify stakeholders
- Broad communications
- Decide isolation strategy
- Preserve forensic data
- IRM (manger) will communicate with management, stakeholders, authorities
- IRM (manger) create an update schedule
- Maintain project tracking

Eradication and Remediation Phase

After an incident has been contained, eradication is necessary to eliminate components of the incident, such as deleting malicious code, disabling breached user accounts or in the case of an intrusion, closing the access path.

Many system born viruses, Trojan-Horses, worms and malicious code events will require an eradication effort such as:

- Restoring systems from clean and non-infected backup
- Rebuilding systems from scratch
- Replacing compromised files with clean versions
- Installing patches
- Changing passwords
- Changing Administration passwords and accounts
- Changing Administration passwords and accounts on firewalls and routers
- Changing the firewall rule sets
- Purging memory or registry files
- DoD wiping of infected hard disks
- Detailed cleaning of Raided disks
- Review and tightening network perimeter security
- Recommendation of adding layer 3 network switches, IPS or additional Firewall's
- Review and imposing higher levels of system logging and auditing
- Insure backup systems and media are clean
- All clear communications

Once an organization or system resource has been successfully attacked, it is often attacked again and again using common threads from past attacks. Long term eradication processes will review the access points of past attacks and secure those areas from further attacks. Then an in-depth review of all backups and data storage systems must be conducted, including databases and user USB drives which are considered data storage devices as well.

Once the systems have been cleaned, network vulnerability scans are required before going back into production. As a precautionary note all systems in the same network segment should be vulnerability scanned as well.

Recovery Phase

The goal of this phase is to put impacted systems back into production in a safe and secure manner as quickly as possible. This means that the system or systems need to be cleaned, tested and verified by the Incident Response Team and approved for operation by a subject matter expert and the IRM (manager).

Requirements

- Follow the recovery procedures
- Document team actions
- Review and insure backups are clean
- Restore user files/data from backups
- All clear communications

Lessons Learned Phase

This is the point at which the system is restored to its normal operating condition. Eradication and recovery have been tested and approved and required software patches have been installed, operational changes have been made through Change Control practices and documented.

It is the responsibility of the IRM (manager).to pull together all the documentation and evidence about the incident and create an Incident Response Report. The draft should contain the artifacts of what occurred during the incident and the remediation processes. Once this report has been created, the IRM (manager) will formally review the information with those that were impacted and participated in handling the incident.

The review will consist of verifying what occurred and discussions about:

- What happened?
- How did it happen?
- Losses or impacted data?
- How can PCC mitigate the risk of a reoccurrence?
- What did the incident handling group do right?
- What did the incident handling group do wrong?
- What can PCC do differently next time?

The Incident Response Team will then compile and submit the final report to management and the Case Management team. Ideally, this will all occur within two weeks of an incident.

Case Management

This is the accumulation of the incident's information, the forensic data, evidence, chain of custody, the people involved and incident summations from the various team leaders. This information is the instrument supporting law suits or protecting the organization from regulatory legal actions. One of the major differences between an incident file and case management file is information that is highly confidential, such as names and addresses, exterior involvements, legal authorities combined with legal documentation and case opinions, will be included in the case management file.

- Low - Incident Response files are required to be stored for 1 year
- All other Incident Response files are required to be stored for 3 years and legal case work may require longer storage requirements.

Training

Each Incident Response Team member shall be trained to a level commensurate with responsibilities of the appointment and consistent with the requirements of PCC IRM (manager) and IRT (team).

For regulatory compliance and certain audits Cyber Security Incident Response drills should be conducted at least quarterly to test the Incident Response Team's training and the approved Incident Response Policy. These tests should range from a paper drill, to a full operational exercise representing an actual incident.

Incident Response Team - IRT

The Incident Response Team (IRT) consists of a Core Team with a Supplemental Team to be called if necessary. Each member of the Primary Team should designate an alternate member to participate if the Primary Member is unavailable. The Primary Team will consist of representatives from the following areas:

Core Team

- Incident Response Manager (IRM) - Val Moreno
- Incident Response Team (IRT)
    - TSS - Information Security Manager (ISM) - Terry Nickerson
    - TSS Campus Managers
    - TSS - Campus Technology Services (CTS)
    - TSS – Application
    - TSS - Network Services

Secondary Team Members (as required)
The circumstances surrounding each incident will differ and require personnel with expertise or skills beyond that of the Primary Team. Members of the Primary Team will determine what, if any, additional resources are required and a Secondary Team may be established with:

- Individuals with decision-making authority identified to have a vested interest in the resolution of the incident.
- Individuals identified as subject matter experts or having skills required for resolution of the incident.
- Information System Managers representing an affected Client or 3rd Party, such as a vendor, may be requested to serve on the Secondary Team.

During an incident the following major units/offices/individuals might be asked to participate in the incident itself and the documentation for an investigation.

Unit/Office/Individual	Area of Responsibility
Deputy Public Safety	Law Enforcement / Criminal Investigation – Ken Goodwin
Miller Nash	Legal Compliance
CIO	Jackie Barretta - 8508
TSS	
Division Manager	Hank Schottland - 8501
Information Security Manager	Terry Nickerson - 4896
Incident Response Manager	Val Moreno - 4390
Network Team Manager	Ed Hawkins - 4394
Server Team Manager	Ben Le - 4736
Applications Team Manager	Joe Cheng - 4165
Web Team Manager	Luis Menchu - 4764
Help Desk Manager	Das Dasgupta – 4415
Campus Manager - Sylvania	Angela McMahon - 4415
Campus Manager - Cascade	Michael Heuer - 4765

Unit/Office/Individual	Area of Responsibility
Campus Manager – South East	Larry Holmberg - 6296
Campus Manager – Rock Creek	Craig Londraville - 7205
Distance Learning	Andy Freed - 8225
Red Flag Team	Dee Wilson - 2844
Red Flag Team	Samantha Hopf - 2804
Red Flag Team	Ken Goodwin - 4980
Red Flag Team	Jody Potter - 7690

Team Objectives

The IRT (team) reports directly to the IRM (manger) . Their combined objective is to:

- Coordinate and oversee the response to Incidents in accordance with the requirements of PCC polices combined with state and federal laws
- Minimize the potential negative impact to the PCC students and staff as a result of such Incidents
- Where appropriate, inform the affected stakeholder(s) of action that is recommended or required on their behalf
- Restore services to a normalized and secure state of operation
- Provide clear and timely communication to all interested parties

Team Responsibilities

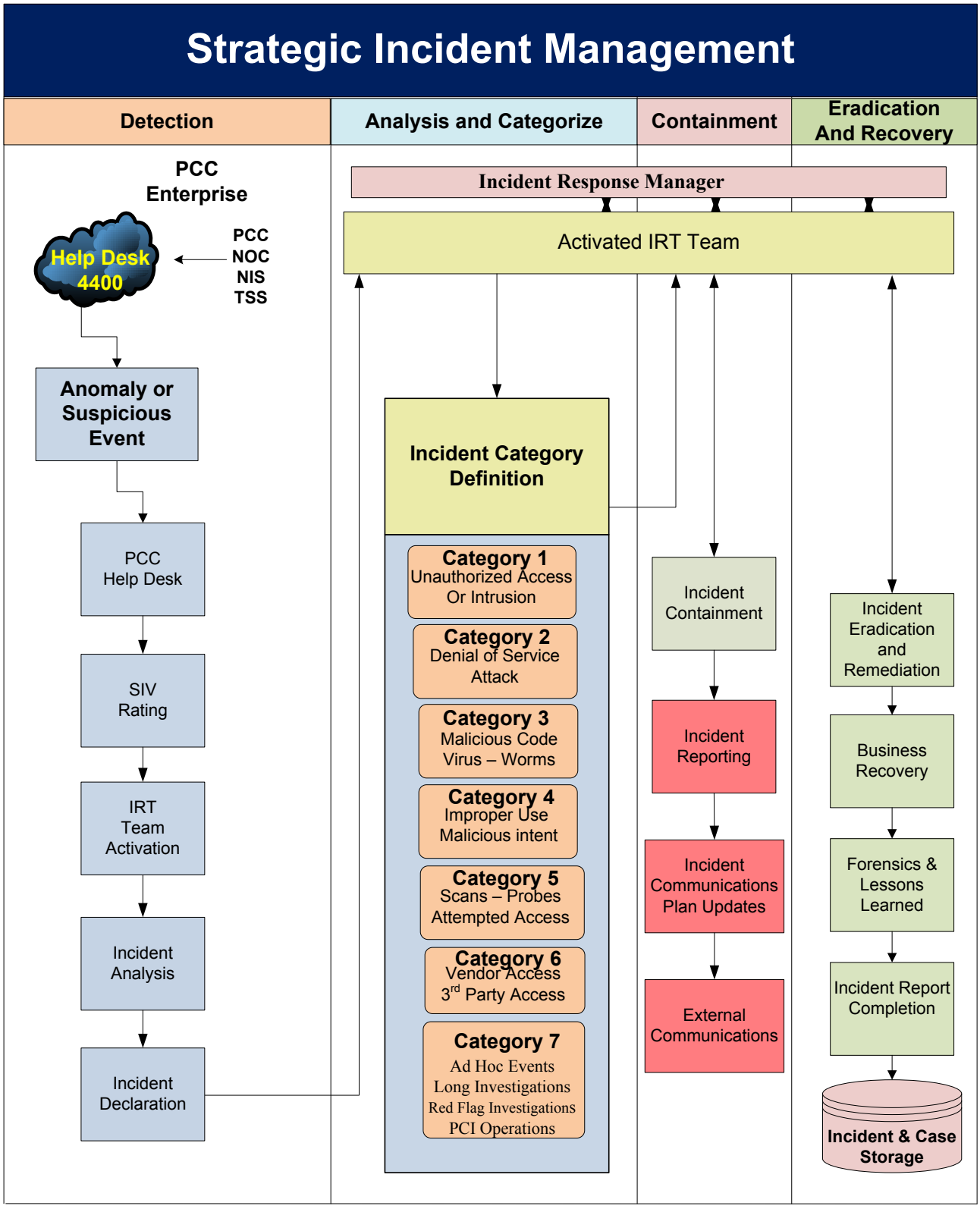
To ensure an appropriate and timely execution of the IRM (manger) directions:

- Confirmation of an Incident requiring the execution of the team
- Confirmation activities include but are not limited to:
    - Direct conversation with Client
    - Communications with the Help Desk
    - Communications with the "on call" manager
    - Communication with IRT (team) members or others having information about the event
    - Updating management about the incident
- A consistent, timely and appropriate response to an Incident
- Provide appropriate communication to parties having a vested interest in the incident
- Offer support to the user groups or community members as appropriate until the Incident is resolved
- Conduct a Lessons Learned Review
- Maintain the procedures contained in this plan

Accountability

Individual IRT members are accountable to the IRM (manger) and PCC Administration for the timely and effective execution of this protocol and associated activities.

Incident Management – Operational Plan



Incident Ranking

The basis of rating systems includes the following rating criteria:

1. The incidents risk exposure to PCC
2. Possible damage
3. Chance of threat granting privileged access
4. Extent the threat is active
5. The recovery aspects
6. Safety of PCC assets
7. Safety of PII and PHI data

Low Ranking Incidents – SIEV Ranking 1 to 2 (on each Factor)

The potential impact is **low** if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

- Cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced
- Result in minor damage to organizational assets
- Result in minor financial loss

PCC uses the following as guidelines when defining a low impact incident:

- Financial – direct or indirect monetary costs to the College where remediation cost is under $10,000
- Reputation – when the impact has a nominal impact on institutional reputation
- Safety – where the impact has nominal impact on safety of campus community members
- Incidents involving systems classified as *Academic*, *Protected*, or *non-essential* are more likely to result in a low impact when considering confidentiality and availability.

Moderate Incidents - SIV Ranking 3 (on at least one Factor)

The potential impact is **moderate** if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

- Cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced
- Result in significant damage to organizational assets
- Result in significant financial loss

PCC uses the following as guidelines when defining a medium impact incident:

- Financial – direct or indirect monetary costs to the College remediation cost is between $10,000 and $100,000
- Reputation – when the impact results in a negative impact on institutional reputation on a local scale
- Safety – when the impact noticeably increases likelihood of injury to community member(s)
- Incidents involving systems classified as *Internal _or _essential* are more likely to result in a moderate impact when considering confidentiality and availability.

High Level Incidents - SIV Ranking 4 (on at least one Factor)

The potential impact is **high** if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might:

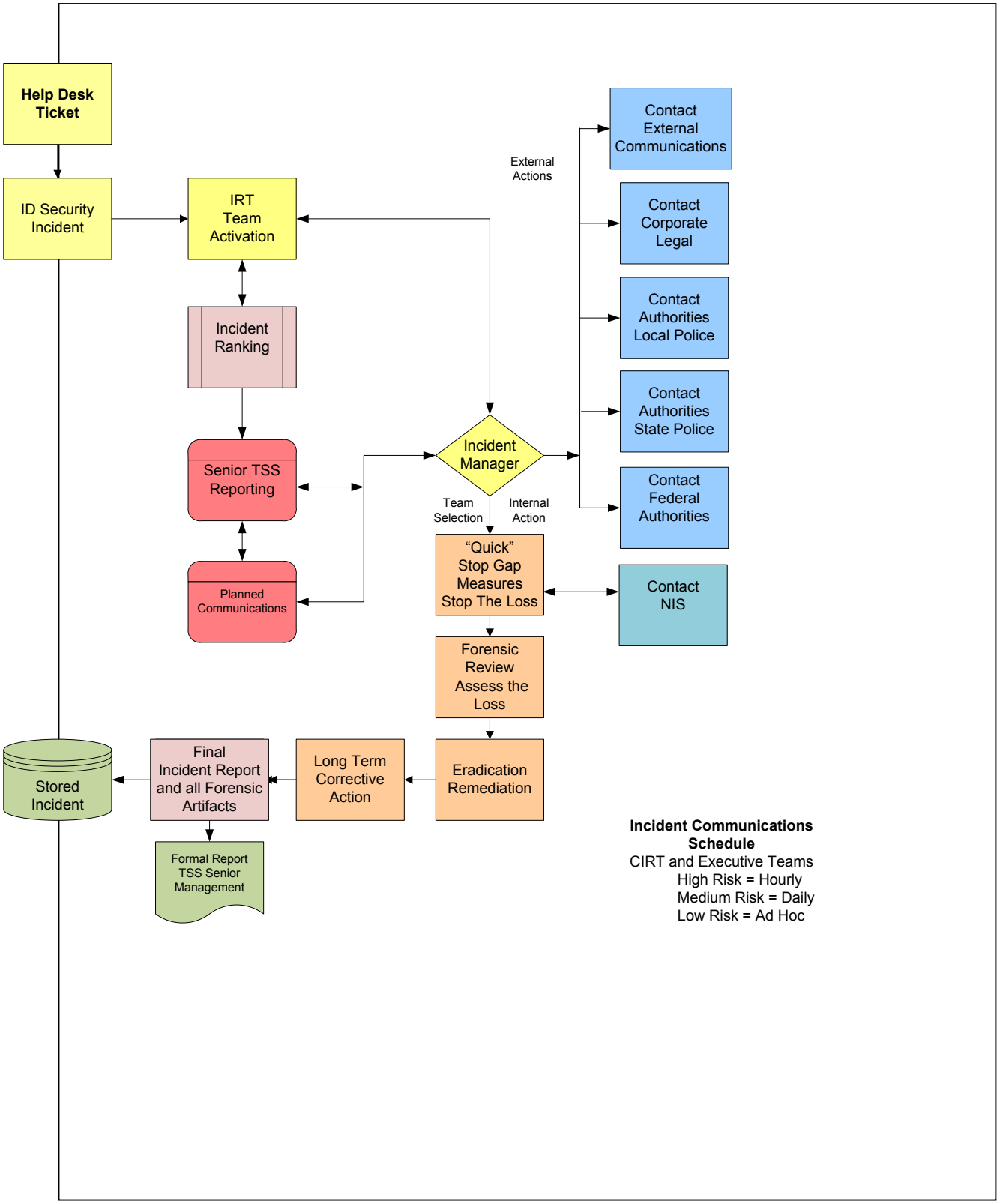
- cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions
- Result in major damage to organizational assets
- Result in major financial loss
- Result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries

PCC uses the following as guidelines when defining a high impact incident:

- Financial – direct or indirect monetary costs to the College where total remediation cost exceeds $100,000
- Reputation – when the impact results in negative impact on institutional reputation on a national or international scale
- Safety – when the impact places campus community members at eminent risk for injury
- Incidents involving systems classified as *private _or _life/safety* are more likely to result in a high impact when considering confidentiality and availability.

Unauthorized Access

Anyone accessing the system for any unauthorized reason is defined as a category 1 attack. Typical attacks might come from janitors, facilities maintenance people, utility repair people or malicious employees. More devious attacks might be off the street people using USB Memory sticks.



Unauthorized Access - Overview

Anyone accessing the system for any unauthorized reason is defined as a category 1 attack. Typical unauthorized attacks might come from off hour people like janitors or facilities maintenance people, utility repair people, malicious employees or unknown hackers. Other attacks could be off the street people using USB Memory sticks or Wi-Fi drive by attacks.

Unauthorized access is typically gained through the exploitation of operating systems, brute force hacking, open vulnerabilities, the acquisition of usernames and passwords through malware, or through social engineering. Examples are;

- Performing a remote root compromise of an email server
- Defacing a Web server
- Guessing or cracking passwords
- Viewing or copying sensitive data, such as payroll records, medical information, and credit card numbers, without authorization
- Running a packet sniffer on a workstation to capture usernames and passwords
- Using a permission error on an anonymous FTP server to distribute pirated software and music files
- Dialing into an unsecured modem and gaining internal network access
- Posing as an executive, calling the help desk, resetting the executive's email password, and learning the new password
- Using an unattended, logged-in workstation without permission
- Deploying a rogue wireless access point to gain internal network access

Gather Forensic Information

- Gather as much ticket information as possible.
- Understand who is trying to or has gained access.
- Identify the systems being exploited

Escalate the Call

Call the technical resources for the threat, application or system and ask for information about the risk level. For all risks factors above low call the event an active incident.

Isolate and Separation of the Affected Systems

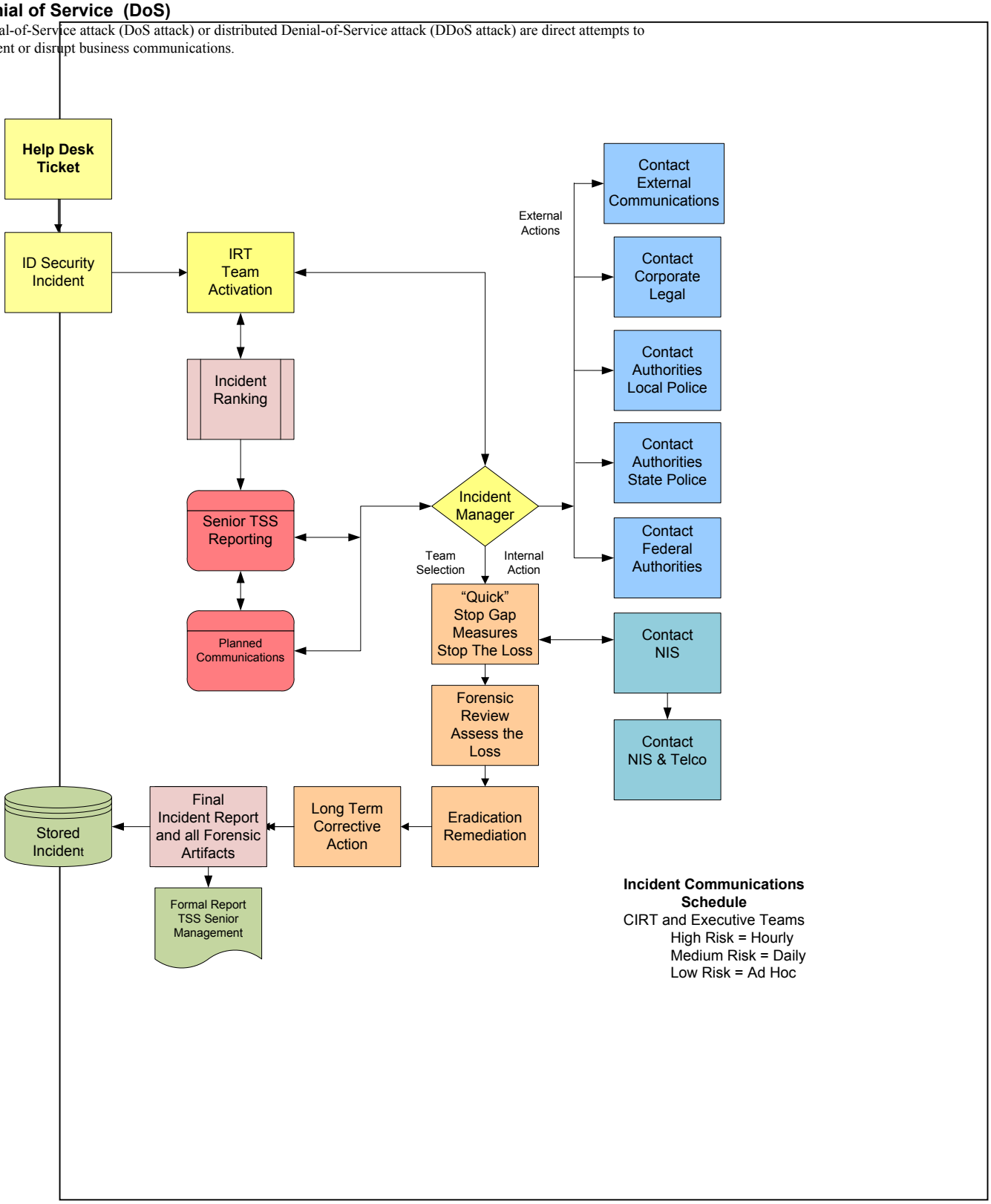
Once the call becomes an incident, ask if isolation is the next step. If approved Isolate the system as quickly as possible. Pulling the network cable is a simplistic and immediate solution for resolving and containing an unauthorized access incident.

The Incident Manager will assume the responsibility of recovery and remediation.

Incident Process Category 2 – Denial of Service Attack (DOS)

Denial of Service (DoS)

Denial-of-Service attack (DoS attack) or distributed Denial-of-Service attack (DDoS attack) are direct attempts to prevent or disrupt business communications.



Incident Communications Schedule

CIRT and Executive Teams
High Risk = Hourly
Medium Risk = Daily
Low Risk = Ad Hoc

Action Plan - Incident Process Category 2

Denial of Service (DoS) - Overview
Denial-of-Service attack (DoS attack) or distributed Denial-of-Service attack (DDoS attack) are direct attempts to prevent or disrupt business communications. Escalate the call to network services (NIS) as quickly as possible.

Gather forensic information
Gather as much ticket information as possible.
Understand who is trying to or has gained access.

Action Plan

- Gather forensic information (try to understand who the attackers are)
- System re-boot – Typically single server DOS or DDOS attacks fill memory and a reboot will resolve the event in the short term. This will not resolve the problem long term.

A denial of service attack (DoS) or (DDOS) is an attack that impairs or prevents the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, communications stack, and disk space. Examples of DoS attacks are;

- Using all available network bandwidth by generating unusually large volumes of traffic
- Sending malformed TCP/IP or UDP packets to a server so that its operating system will crash
- Sending illegal requests to an application to crash it
- Making many processor-intensive requests so that the server's processing resources are fully consumed
- Establishing many simultaneous login sessions to a server so that other users cannot start login sessions
- Broadcasting on the same frequencies used by a wireless network to make the network unusable
- Consuming all available disk space by creating many large files.

For most organizations, including PCC, network bandwidth is so large that a single attacking machine cannot cause a network DoS. Instead, attackers perform distributed denial of service (DDoS) attacks, which coordinates an attack across many computers. If enough hosts are used, the total volume of generated network traffic can consume not only the resources of a targeted host but also the available bandwidth for other PCC applications. As criminal technology has grown DDoS attacks have become an increasingly severe threat. With web servers down the lack of availability of computing and network services causes significant disruption and major financial loss. No organization is completely safe from DDoS attacks but incident response plans can help in two ways, first, knowing the attack is underway technology engineers can react and recover. Second, engineers can gather forensic information and the capability of prosecuting the attackers is very real.

Type of Attack - Reflector DoS Attacks
In a reflector attack, a host sends many requests with a spoofed source address to a service on an intermediate host. The service used is typically User Datagram Protocol (UDP) based, but can be TCP/IP as well, which makes it easier to spoof the source address successfully. Attackers often use spoofed source addresses because they hide the actual source of the attack. That host generates a reply to each request and sends these replies to the spoofed address. Because the intermediate host unwittingly performs the attack, that host is known as a reflector. During a reflector attack, a DoS could occur to the host at the spoofed address, the reflector itself, or both hosts.

Type of Attack - Amplifier Attacks
Like a reflector attack, an amplifier attack involves sending requests with a spoofed source address to an intermediate host. However, an amplifier attack does not use a single intermediate host, instead, its goal is to use a whole network of intermediate hosts. It attempts to accomplish this action by sending an ICMP or UDP request to an expected broadcast address, hoping that many hosts will receive the broadcast and respond to it. Because the attacker's request uses a spoofed source address, the responses are all sent to the spoofed address, which may cause a DoS for that host or the host's network. Most environments block amplifier attacks by configuring border routers to not forward directed broadcasts, but some still permit them.

Type of DOS Attacks - Flood Attacks
A DDoS attack that makes a resource unavailable by initiating large numbers of incomplete connection requests is considered a flood attack. This type of attack overwhelms capacity, typically preventing new connections from being made. Flood attacks can occur using many different methods resulting in DDoS. One example is a peer-to-peer attack, which involves an attacker disconnecting a peer-to-peer file sharing hub from its peer-to-peer networks and redirecting traffic to a victim's Web site. When thousands of computers to try to connect to what they think is the file sharing hub, the victim's Web server becomes overwhelmed, causing it to fail.

Another example of a flood attack is a synflood, which occurs when an attacker initiates many TCP connections in a short time by sending SYN packets but does not complete the TCP three-way handshakes necessary to fully establish each connection.

DOS and DDoS - Incident Prevention
The following items provide additional recommendations for preventing DoS incidents:

- Configure the network perimeter to deny all incoming and outgoing traffic that is not expressly permitted.
- Blocking the usage of services, such as echo
- Performing egress and ingress filtering to block obviously spoofed packets.
- Blocking traffic from unassigned IP address ranges, known as bogon lists.
- Configuring border routers not to forward directed broadcasts.

- Limiting incoming and outgoing ICMP traffic to only the necessary types and codes.
- Blocking outgoing connections to common IRC, peer-to-peer service and instant messaging ports if the usage of such services is not permitted.
- Implement rate limiting for certain protocols, such as ICMP, so that they can only consume a designated percentage of the total bandwidth. Rate limiting can be implemented at the organization's network perimeter, border routers and firewalls.
- On Internet-accessible hosts, disable all unneeded services, and restrict the use of services that may be used in DoS attacks, configure DNS servers so they do not permit recursion
- Ensure that networks and systems are not running near maximum capacity

DOS and DDoS - Detection and Analysis

DoS and DDoS attacks pose some additional challenges in terms of incident analysis:
DoS attacks often use connectionless protocols (UDP and ICMP) or use a connection-oriented protocol in such a way that full connections are not established (e.g., sending TCP SYN packets to create a synflood attack). Therefore, it is relatively easy for attackers to use spoofed source IP addresses, making it difficult to trace the source of attacks. ISPs may be able to assist in tracing the activity, but it is often more effective to review logs for previous reconnaissance activity that appears to be related. Because the attacker would want to receive the results of the reconnaissance, such activity is unlikely to use a spoofed address, so it may indicate the location of the attacker.

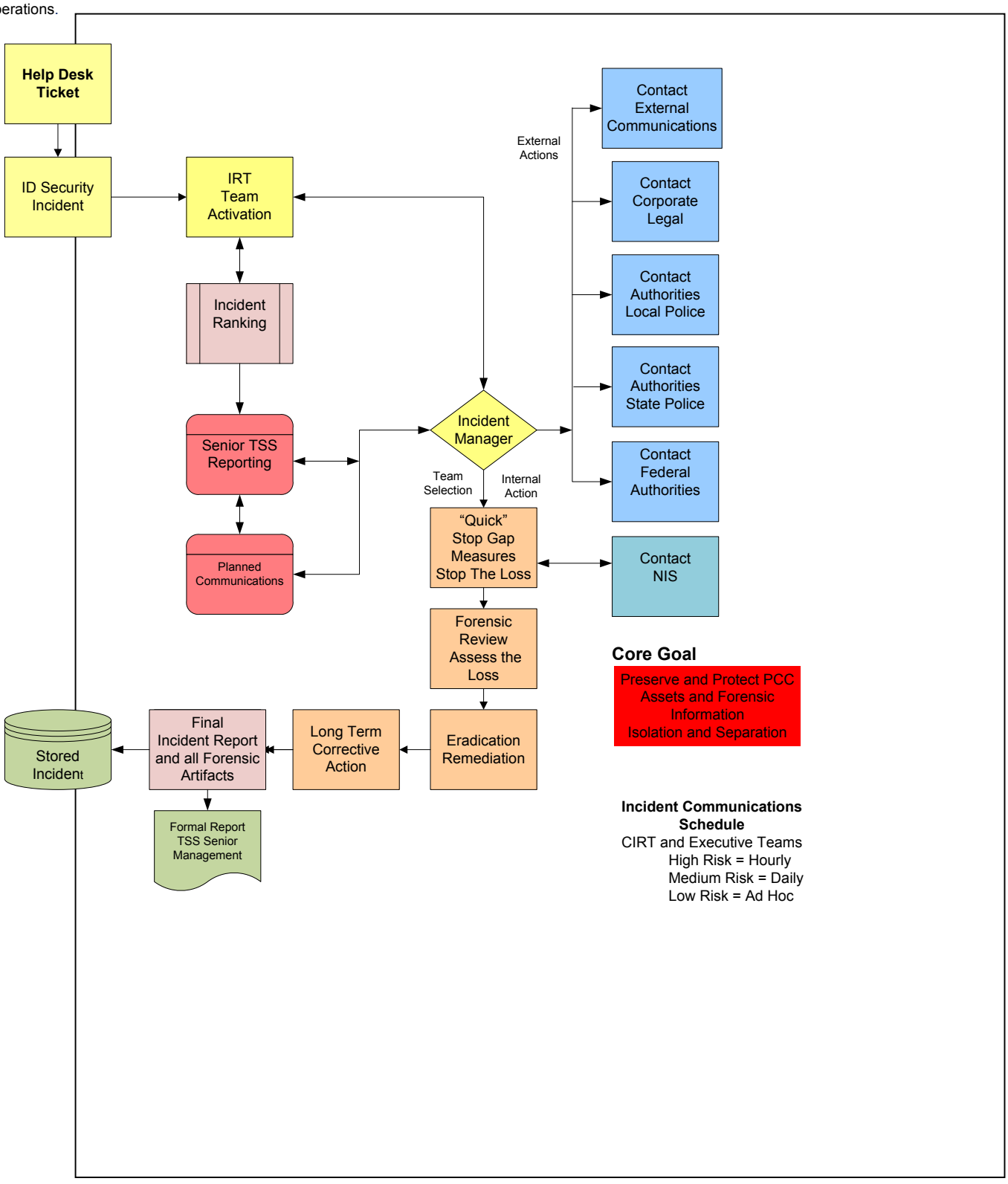
DDoS attacks often use thousands of workstations that are controlled by a single handler (or no handler at all). These workstations usually have bots installed that are considered "zombies" and are activated by the controller to attack other systems. The victim site will not see the IP of the handler, and even if it could, it is likely that it is just another host that the attacker has compromised.

Network-based DoS attacks are difficult for IDS/IPS sensors to detect with a high degree of accuracy. For example, synflood alerts are one of the most common false positives in network IDS/IPS products. If an attacker performs a rapid SYN scan, many IDS/IPS products will report it as a synflood, even though the activity is sending only one request to each port. If a server crashes, hosts trying to reconnect to it may keep sending SYN packets. Sometimes many legitimate connections in a short time (e.g., retrieving many elements of a Web page) will also cause a synflood alert to be triggered.

When an outage occurs, no one may realize that a DoS attack caused it. For example, a Web server may crash occasionally as a result of operating system instability, requiring a reboot for its functionality to be restored. If an attacker sends some specially crafted packets to the Web server that cause it to crash, system administrators may assume the crash resulted from the operating system's instability and not realize that an attack took place.

Incident Process Category 3 – Malicious Code

Malicious Code
Most computer users understand malicious code called viruses, worms or Trojan horses. Malicious software is designed to infiltrate or damage a computer system without the owner or operators approval or permission. This type of software is considered malware because its sole purpose is to disrupt business operations.



Action Plan - Incident Process Category 3

Malicious Code – Over View
Malicious code refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the security or the confidentiality, integrity, and availability of the victim's data, applications, or operating system. Generally, malicious code is designed to perform these nefarious functions without the system's user knowledge. There are many categories of malicious code, spread across a few general categories akin to viruses, worms, Bots (programmable robots), Trojan horses, spyware, malicious mobile code, and blended attacks. Malware also includes attacker tools such as backdoors, rootkits, and keystroke loggers, and tracking cookies used as spyware.

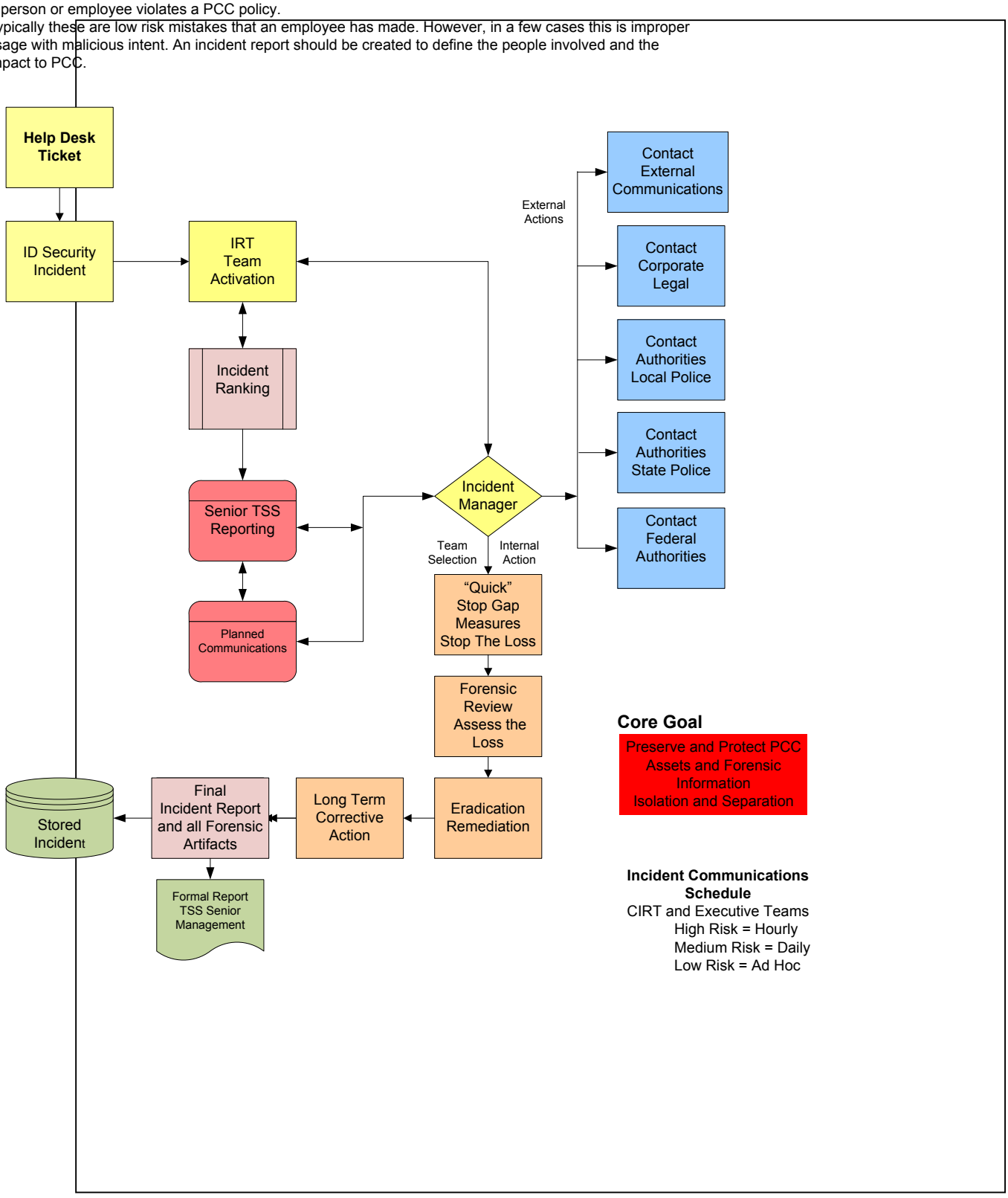
Gather forensic information

- Gather as much ticket information as possible.
- Understand who is trying to or has gained access.
- Run Malwarebytes on the system and document the review
- Review all logs and save the forensic information.

Action Plan
Isolation and separation processes. Separate the system from the network by unplugging the network cable. Leave the system powered on to preserve the forensic information and limit all access points. For example, block all users from logging into the system until the research is complete.

Incident Response
Improper Use

Improper Use
A person or employee violates a PCC policy.
Typically these are low risk mistakes that an employee has made. However, in a few cases this is improper usage with malicious intent. An incident report should be created to define the people involved and the impact to PCC.



Core Goal

Preserve and Protect PCC Assets and Forensic Information
Isolation and Separation

Incident Communications Schedule
CIRT and Executive Teams
High Risk = Hourly
Medium Risk = Daily
Low Risk = Ad Hoc

Action Plan – Incident Process Category 4

Improper Use
A person or employee violates a PCC policy. Typically these are low risk mistakes that an employee has made. If minor, at this level an incident report is not required. Purposeful or malicious improper usage is different and an incident report should be created, filed and reported.

Gather forensic information

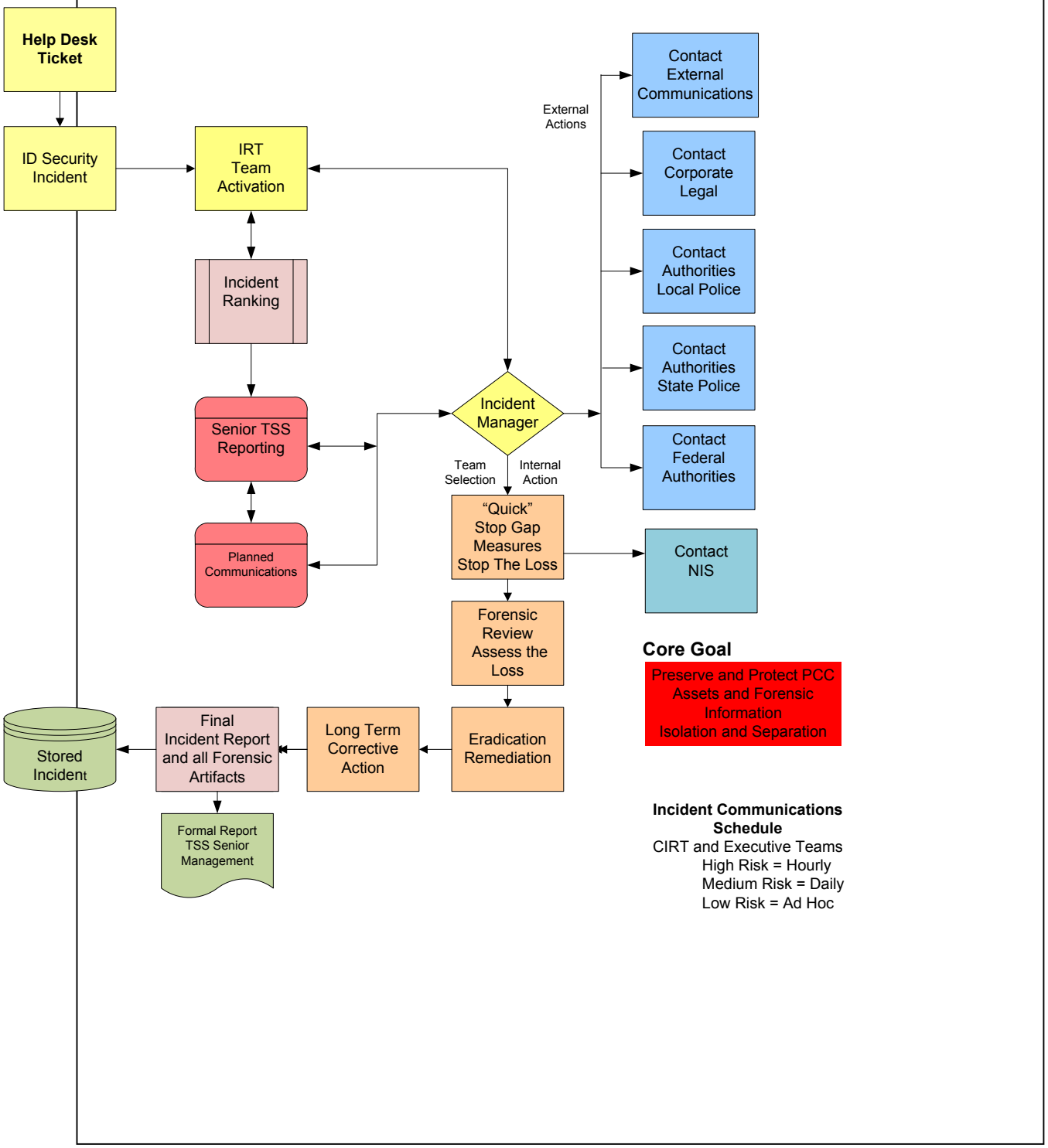
- Gather as much ticket information as possible.
- Understand who is trying to or has gained access.
- Review all logs and save the forensic information.

Action Plan
Isolation and separation processes. Separate the system from the network by unplugging the network cable. Leave the system powered on to preserve the forensic information and limit all access points.

Incident Response
Scans – Probes – Attempted Access

Scans – Probes – Attempted Access

This includes any activity that seeks to access and identify operating systems, system ports, protocols and available system resources. Because scans and probes can be a preliminary process to an intrusion or system access an incident file should be created and acted on quickly, time is critical in these situations. Intrusion are a much higher risk to PCC and require immediate escalation.



Action Plan – Incident Process Category 5

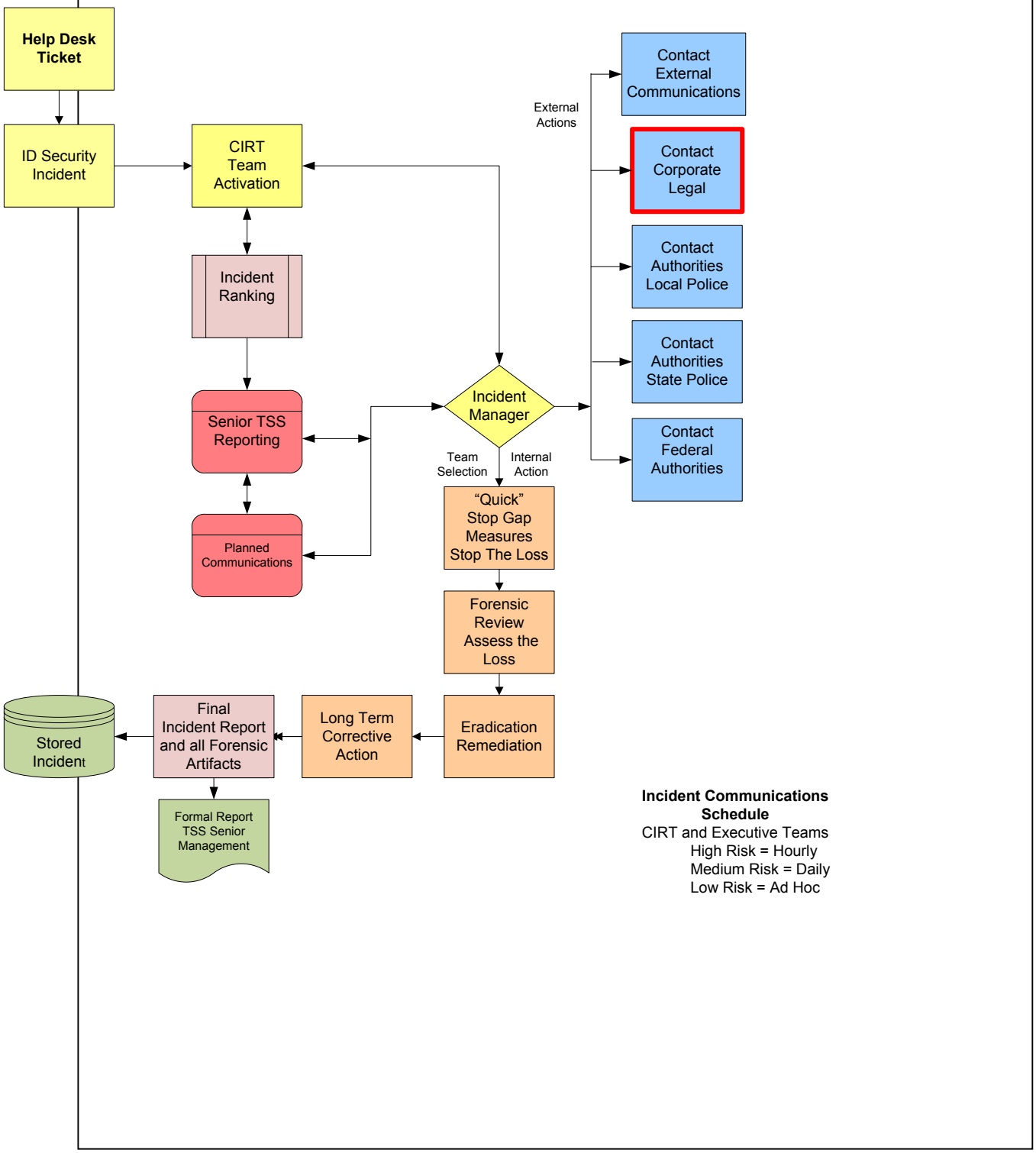
Scans – Probes – Attempted Access
This includes any activity that seeks to access and identify operating systems, system ports, protocols and available system resources. Because scans and probes can be a preliminary process to an intrusion or system access, an incident file should be created, reviewed and stored. Intrusions are a much higher risk and require immediate containment and escalation.

Gather forensic information
Gather as much ticket information as possible.
Understand who is trying to or has gained access.
Review all logs and save the forensic information.

Action Plan
Isolation and separation processes. Separate the system from the network by unplugging the network cable. Leave the system powered on to preserve the forensic information, and limit all access points. Advise the IRM manager to implement immediate incident escalation procedures.

Incident Process Category 6 – Vendor Access

Vendor or 3rd Party Access
Most organizations invite 3rd party vendors into their network for maintenance, service or patch updates. Third party organizations are also allowed to freely access systems to transfer information, place an order, check inventory and authorize payments. During this access sensitive data could be viewed, copied or touched in some manner.



Incident Communications Schedule
CIRT and Executive Teams
High Risk = Hourly
Medium Risk = Daily
Low Risk = Ad Hoc

Action Plan - Incident Process Category 6

Vendor or 3rd Party Access
Most organizations invite key software vendors into their system for maintenance, service or patch updates. Organizations also grant 3rd party organizations access to their systems to transfer information, place an order, check inventory and authorize payments. During this access, sensitive information could be viewed or touched in some manner.

Gather forensic information

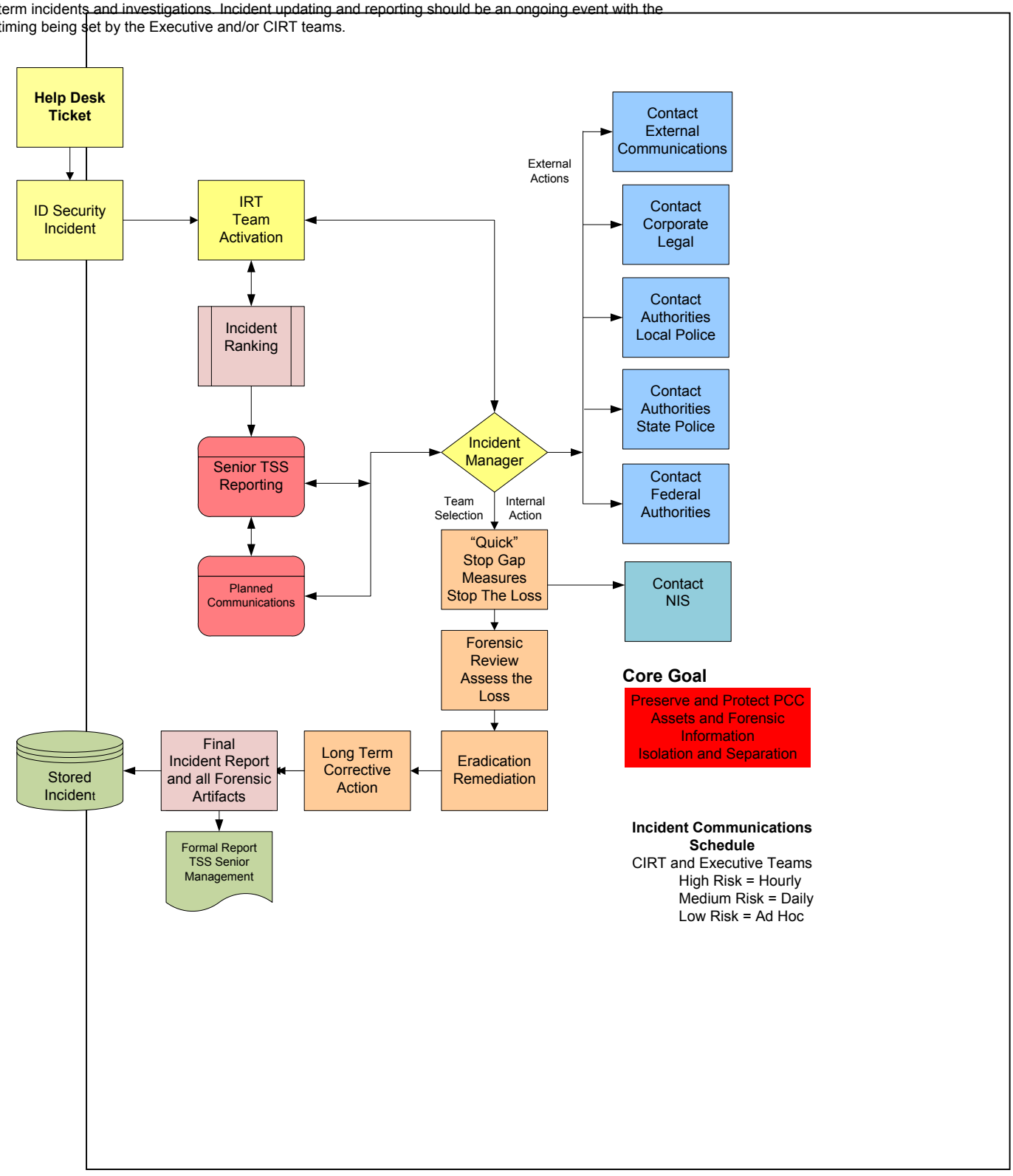
- Gather as much ticket information as possible.
- Understand who is trying to or has gained access.
- Review all logs and save the forensic information.

Action Plan
Isolation and separation processes. Separate the system from the network by unplugging the network cable. Leave the system powered on to preserve the forensic information, and limit all access points.

Incident Process Category 7 – Ad Hoc – Long Term - PCI

Ad Hoc Events and Long Term Investigations

Ad Hoc system or application problems may be a precursor to malicious inference or a virus, worm or Trojan. These can be difficult long term events to detect and resolve. Category 7 is parking space for longer term incidents and investigations. Incident updating and reporting should be an ongoing event with the timing being set by the Executive and/or CIRT teams.



Action Plan - Incident Process Category 7

Ad Hoc Events - Long Term Events - Red Flag Investigations or PCI Operations

Ad Hoc system or application problems may be a precursor to malicious interference or a virus, worm or Trojan. These can be long term events to resolve. Category 7 is parking space for longer term case investigations involving technology, malicious acts or fraud. Incident updating and reporting should be an ongoing event with the timing being set by the IRT team.

Gather forensic information

- Gather as much ticket information as possible.
- Understand who is trying to or has gained access.
- Review all logs and save the forensic information.

Action Plans

Ad Hoc Events will require special attention and an out of scope focus for everyone involved. Keep the IRM manager informed of the details and if the events is serious document the details as they occur.

Long Term Events are incidents or events that will require a longer term for reporting and recovery, but not long enough to become a project.

PCI Operations and Events - To address credit cardholder security, the major credit card brands have mutually agreed to establish the PCI/DSS Security Standards Council to administer the Payment Card Industry.

The PCI Response Team is a very specific team geared towards protecting cardholder information, the cardholder and the systems supporting that information. The IRM manager will investigate the incident and assist potentially compromised cardholders and in mitigating the risks associated with the incident.

The IRM manger will focus the PCI Response Team in resolve the problem to the satisfaction of all parties involved.

Quarterly, the PCI Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution.

Action Plan - PCI Incident

After being notified of an incident or system compromise, the IRM manager will convene the PCI Response Team, coupled with other designated staff, to assist and support the response plans.

The first and most immediate step is to isolate and separate the systems from the network. Separate the system from the network by unplugging the network cable. Leave the system powered on to preserve the forensic information, and limit all access points.

Assimilate review and analyze the event information then conduct appropriate internal and external reviews documenting the case.

Incident or Threat Enforcement

Student Incident Involvement

Student disciplinary procedures are covered in the Student Rights and Responsibilities Handbook.

Employee Incident Involvement

If an employee is identified as the source of an incident it is essential to notify Human Resources and the Help Desk as soon as possible. The IRM manager will provide information and recommendations to HR.

Classified professional disciplinary procedures are covered in Article 21 Discipline and Dismissal.

Academic professional disciplinary procedures are covered in Article 22 Discipline and Dismissal of the Faculty and Academic Professional Agreement.

Disciplinary procedures for managers and confidential staff are covered in the Management and Confidential Employee Handbook.

External Incident Involvement

In the case of an external threat the escalation process should be handled by the IRM (manager) and possibly PCC Public Safety. If required and approved by the IRM (manager) PCC Public Safety Office will respond by taking appropriate action(s) to identify, apprehend, and seek prosecution of the person(s) responsible.

Public Safety is the authorized liaison to law enforcement. Direct reporting to law enforcement can be a liability since Public Safety is trained to facilitate support of emergency services. As an example, if a serious event occurs on a campus and law enforcement is needed, Public Safety would meet with emergency services and escort them to the proper location.

If an incident is serious enough, campus/district notification may be necessary. This role is facilitated by Public Safety to Institutional Advancement (public relations), Flash Alert, e911, and/or Campus Notification Systems.

In the case of a severe incident, activation of the Emergency Operations Plan may be required.

Unintentional Incident Involvement

The vast majority of incidents are the result of a lack of training and awareness, a first responder can coach the user/patron on the spot. It is often helpful to contact the area supervisor to inform them of the incident. This may help identify re-occurring issues and identify training needs.

The IRM (manager) may recommend escalation procedures.

Contact Information

Help Desk and Incident Reporting 971-722-4400
PCC Public Safety 971-722-4444

Incident Response Team Members

Contact Name	Title or Position	Office Phone	Cell Phone	E-Mail
Val Moreno	Division Manager	971-722-4390	312-909-7911	val.moreno@pcc.edu
Terry Nickerson	Information Security Manager	971-722-4896	971-285-2727	Terry.Nickerson@PCC.edu
Ed Hawkins	Network Manager	971-722-4394	702-498-6820	ed.hawkins@pcc.edu
Joe Cheng	Applications Manager	971-722-4165	503-786-0364	jcheng@pcc.edu
Luis Menchu	Web App Manager	971-722-4764	503-969-4028	lmenchu@pcc.edu
Mike Arnold	Banner Manner	971-722-4326	503-936-5427	marnold@pcc.edu
Ben Le	Server Manager	971-722-4736	503-334-6936	ble@pcc.edu

General Contacts

Contact Name	Title or Position	Office Phone	Cell Phone	E-Mail
Angela McMahon	Sylvania Campus Manager	971-722-4415	503-577-1613	amcmahon@pcc.edu
Craig Londraville	Rock Creek Campus Manager	971-722-7205	503-941-0522	craig.londraville@pcc.edu
Michael Heuer	Cascade Campus Manager	971-722-4765	360-521-1042	michael.heuer@pcc.ed
Larry Holmberg	SE Campus Manager	971-722-6296	503-957-1578	lholmber@pcc.edu
Das Dasgupta	Help Desk Manager	971-722-7876	503-522-9201	das.dasgupta@pcc.edu

Senior Management

Contact Name	Title or Position	Office Phone	Cell Phone	E-Mail
Sylvia Kelly	PCC President	971-722-4365		sylvia.kelley@pcc.edu
Jackie Barretta	CIO		503-810-6171	jackie.barretta15@pcc.edu
Hank Schottland	Division Manager	971-722-8501	503-969-6774	hank.schottland@pcc.edu
Val Moreno	Division Manager	971-722-4390	312-909-7911	val.moreno@pcc.edu

References – Organizations – Tools

Aspects of this Policy and Plan were derived from the following reference resources. Bolded references contributed a larger information share.

These references are included to support an active incident or investigation. A local repository is recommended to store reference materials in case of an Internet Outage.

Supporting Incident Response Information
Computer Crime and Intellectual Property Section (CCIPS), U.S. Department of Justice
http://www.cybercrime.gov/

CERT® Coordination Center, Carnegie Mellon University (CERT®/CC)
http://www.cert.org/

CERT®/CC Incident Reporting System
https://irf.cc.cert.org/

Computer Incident Advisory Capability (CIAC), U.S. Department of Energy
http://www.ciac.org/ciac/

Forum of Incident Response and Security Teams (FIRST)
http://www.first.org/

Government Forum of Incident Response and Security Teams (GFIRST)
http://www.us-cert.gov/federal/gfirst.html

High Technology Crime Investigation Association (HTCIA)
http://www.htcia.org/

IETF Extended Incident Handling (inch) Working Group
http://www.cert.org/ietf/inch/inch.html

InfraGard
http://www.infragard.net/

Internet Storm Center (ISC)
http://isc.incidents.org/

United States Computer Emergency Response Team (US-CERT)
http://www.us-cert.gov/

US-CERT Incident Reporting System
https://forms.us-cert.gov/report/

Forensics
http://www.securityfocus.com/archive/104

Incidents
http://www.securityfocus.com/archive/75

Log Analysis
http://www.loganalysis.org/pipermail/loganalysis/

Cyber Alerts
National Cyber Alert System
http://www.us-cert.gov/cas/

Technical Cyber Security Alerts
http://www.us-cert.gov/cas/techalerts/

Cyber Security Alerts
http://www.us-cert.gov/cas/alerts/

Cyber Security Bulletins
http://www.us-cert.gov/cas/bulletins/

Cyber Security Tips
http://www.us-cert.gov/cas/tips/

Current Activity
http://www.us-cert.gov/current/

Computer Security Resource Center (CSRC), NIST
http://csrc.nist.gov/

Incident Handling Links and Documents

National Institute of Justice (NIJ) Electronic Crime Program
http://www.ojp.usdoj.gov/nij/topics/technology/electronic-crime/welcome.htm

NIST Internet Time Service
http://tf.nist.gov/service/its.htm

SANS Institute Reading Room
http://www.sans.org/reading_room/

Security Focus
http://www.securityfocus.com/

Vulnerability and Exploit Information Resources

CERT®/CC Advisories
http://www.cert.org/advisories/

CERT®/CC Incident Notes
http://www.cert.org/incident_notes/

CERT®/CC Vulnerability Notes Database
http://www.kb.cert.org/vuls/

CIAC Bulletins
http://www.ciac.org/ciac/bulletins.html

Common Vulnerabilities and Exposures (CVE)
http://cve.mitre.org/

National Vulnerability Database (NVD)
http://nvd.nist.gov/

Open Vulnerability Assessment Language (OVAL)
http://oval.mitre.org/

Packet Storm
http://www.packetstormsecurity.com/

SANS Top 20 Security Risks List
http://www.sans.org/top20/

SecurityFocus Vulnerabilities Database
http://www.securityfocus.com/bid/

Other Technical Resource Documents

CIO Cyberthreat Response and Reporting Guidelines
http://www.cio.com/research/security/incident_response.pdf

Computer Security Incident Response Planning
http://documents.iss.net/whitepapers/csirplanning.pdf

Computer Security Incident Response Team (CSIRT) Frequently Asked Questions (FAQ)
http://www.cert.org/csirts/csirt_faq.html

Denial of Service Attacks
http://www.cert.org/tech_tips/denial_of_service.html

Electronic Crime Scene Investigation: A Guide for First Responders
http://www.ncjrs.gov/pdffiles1/nij/187736.pdf

Handbook for Computer Security Incident Response Teams (CSIRTs)
http://www.cert.org/archive/pdf/csirt-handbook.pdf

How to Design a Useful Incident Response Policy
http://www.securityfocus.com/infocus/1467

Incident Management Capability Metrics, Version 1.0
http://www.cert.org/archive/pdf/07tr008.pdf

Incident Response: Managing Security at Microsoft
http://www.microsoft.com/downloads/details.aspx?familyid=36e889be-4fb0-447a-943a-7484cba0e7c1&displaylang=en

Incident Response Tools for Unix, Part One: System Tools
http://www.securityfocus.com/infocus/1679

Incident Response Tools for Unix, Part Two: File-System Tools
http://www.securityfocus.com/infocus/1738

Managing the Threat of Denial-of-Service Attacks
http://www.cert.org/archive/pdf/Managing_DoS.pdf

OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information
http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf

Responding to Intrusions
http://www.sei.cmu.edu/pub/documents/sims/pdf/sim006.pdf

RFC 2350: Expectations for Computer Security Incident Response
http://www.ietf.org/rfc/rfc2350.txt

RFC 3067: TERENA's Incident Object Description and Exchange Format Requirements
http://www.ietf.org/rfc/rfc3067.txt

RFC 3227: Guidelines for Evidence Collection and Archiving
http://www.ietf.org/rfc/rfc3227.txt

RFC 4732: Internet Denial-of-Service Considerations
http://www.ietf.org/rfc/rfc4732.txt

RFC 5070: The Incident Object Description Exchange Format
http://www.ietf.org/rfc/rfc5070.txt

Sample Incident Handling Forms, SANS Institute
http://www.sans.org/incidentforms

Staffing Your CSIRT—What Basic Skills Are Needed?
http://www.cert.org/csirts/csirt-staffing.html

A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms
http://lasr.cs.ucla.edu/ddos/ucla_tech_report_020018.pdf

Knowledge Base Resources

IANA Protocol Numbers and Assignment Services
http://www.iana.org/protocols/

Domain Name System Parameters
http://www.iana.org/assignments/dns-parameters

ICMP Type Numbers
http://www.iana.org/assignments/icmp-parameters

Internet Multicast Addresses
http://www.iana.org/assignments/multicast-addresses

Internet Protocol V4 Address Space
http://www.iana.org/assignments/ipv4-address-space

IP Protocol Numbers
http://www.iana.org/assignments/protocol-numbers

IP Version Numbers
http://www.iana.org/assignments/version-numbers

Port Numbers
http://www.iana.org/assignments/port-numbers

Syslog Parameters
http://www.iana.org/assignments/syslog-parameters

TCP Header Flags
http://www.iana.org/assignments/tcp-header-flags

TCP Option Numbers
http://www.iana.org/assignments/tcp-parameters

IETF RFCs for Common Protocols (DNS, FTP, HTTP and SMTP)
http://www.ietf.org/rfc.html

RFC 959: File Transfer Protocol (FTP)
http://www.ietf.org/rfc/rfc0959.txt

RFC 1034: Domain Names—Concepts and Facilities
http://www.ietf.org/rfc/rfc1034.txt

RFC 1035: Domain Names—Implementation and Specification
http://www.ietf.org/rfc/rfc1035.txt

RFC 2065: Domain Name System Security Extensions
http://www.ietf.org/rfc/rfc2065.txt

RFC 2228: FTP Security Extensions
http://www.ietf.org/rfc/rfc2228.txt

RFC 2616: Hypertext Transfer Protocol—HTTP/1.1
http://www.ietf.org/rfc/rfc2616.txt

RFC 2617: HTTP Authentication: Basic and Digest Access Authentication
http://www.ietf.org/rfc/rfc2617.txt

RFC 2821: Simple Mail Transfer Protocol
http://www.ietf.org/rfc/rfc2821.txt

RFC 2822: Internet Message Format
http://www.ietf.org/rfc/rfc2822.txt

Ports-Official and Unofficial Port Assignments
http://ports.tantalo.net/

Incident Management
PCC Lessons Learned

Part of resolving an incident is a lessons learned element which can be utilized time and time again. This section is intended to be a living chapter being updated with lessons learned after each cyber incident.

Personal Computer - Laptop Theft

After receiving report that a laptop is missing Help Desk procedure is to:

1. Check with Laptop owner if they had a theft report completed with local Law enforcement. Computrace requires the report number along with Police agency name, the Precinct, Officer's name and phone number before we can file the stolen device report.
2. Look up as much information about the missing laptop in KBOX and Computrace, the most useful information needed will be device name, serial number, make, model, and user name.
3. After gathering the information Help Desk staff will create a Service Desk work order with all the information from KBOX and Computrace.
4. Assign the Service Desk work order to Information Security Manager, with a task to the appropriate Campus Technology Manager, Public Safety, TSS Customer Support Manager, and Help Desk.
5. Create an incident status Email listing the laptop's information and Service Desk work order number to, Information Security Manager, Campus Manager, Public Safety, TSS Customer Support Manager, Help Desk and laptop owner.
6. After the Information Security Manager completes their process, Help Desk will complete the Computrace stolen device report. Recovery@Absolute will E-Mail Help Desk a Confirmation ID number of the completed report.
7. If a data delete is authorized by management, Help Desk technician will request from Computrace an Authorization Code. To do this, Log into your Computrace account, Navigate to Data and Device Security, > Security Authorization,> Request Authorization Code,> Click on Request Code. You will receive an authorization code via E-Mail, this code is only valid for two hours from the time it is issued.
8. To use the authorization Code, navigate to Data and Device Security,> Data Delete,> request Data Delete page, and complete the Data Delete request.
9. After submitting the data delete request, Help Desk will receive a confirmation Email from recovery@absolute.com.

Unauthorized Access

Anyone accessing the system for any unauthorized reason is defined as a category 1 attack. Typical unauthorized attacks might come from off hour people like janitors or facilities maintenance people, utility repair people, a student or malicious employees. More devious attacks are off the street using USB Memory sticks, drive by attacks or brute force attacks.

Unauthorized access is typically gained through the exploitation of operating systems, brute force hacking, open vulnerabilities, the acquisition of usernames and passwords, or through social engineering. Examples are:

- Performing a remote root compromise of a server
- Defacing a Web server or service
- SQL Injection
- Guessing or cracking passwords
- Viewing or copying sensitive data, such as payroll records, medical information, and credit card numbers, without authorization
- Running a packet sniffer on a workstation to capture usernames and passwords
- Using a permission error on an anonymous FTP server to distribute pirated software and music files
- Dialing into an unsecured modem and gaining internal network access
- Posing as an executive, calling the help desk, resetting the executive's email password, and learning the new password
- Using an unattended, logged-in workstation without permission
- Promoting authentication rights

Action Plan

Gathering forensic information

Understand who is trying to or has gained access.
Review all logs and save the forensic information.

System Reboot

A reboot will break an active connection and reset the system parameters. This is a temporary solution, typically the attacker will be back.

Apply System Monitoring
Continue to review the system and attempt to discover the attacker.

Isolate the affected systems.
Pulling the network cable is a simplistic solution for resolving and containing an unauthorized access incident. While this does prevent the affected systems from being further compromised, it also renders the system un-operational.

Disable the affected service.
If an attacker is using a particular service to gain unauthorized access, containing the incident may include temporarily or permanently disabling the service. For example, if the attacker is exploiting an FTP vulnerability and the unauthorized access is limited to the FTP data files, the incident could be contained by temporarily disabling the FTP service. If the server is inadvertently running FTP, then FTP should be disabled permanently.

Eliminate the attacker's logical route into the environment.
Review the network access route and prevent the attacker from gaining access to the system. Adding a network firewall or adding layer 3 switches may resolve the problem, depending on how sophisticated the attacker is.

Change or Disable user accounts that may have been used in the attack.
Passwords, accounts and Active Directory access must be reviewed and changed. Expired user accounts must be disabled and system administration password must be changed.

Enhance physical security measures.
If an unauthorized access incident was involved with the breach of physical security, additional containment and intruder strategies must be reviewed.

Denial of Service Attack

Denial-of-Service attack (DoS attack) or distributed Denial-of-Service attack (DDoS attack) are direct attempts to prevent or disrupt business communications.

Action Plan

- Gather forensic information (try to understand who the attackers are)
- System re-boot – Typically single server DOS or DDOS attacks fill memory and a reboot will resolve the event in the short term. This will not resolve the problem long term.

Technology Guidance

NIST 800-61

A denial of service attack (DoS) or (DDOS) is an attack that impairs or prevents the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, communications stack, and disk space. Examples of DoS attacks are:

- Using all available network bandwidth by generating unusually large volumes of traffic
- Sending malformed TCP/IP or UDP packets to a server so that its operating system will crash
- Sending illegal requests to an application to crash it
- Making many processor-intensive requests so that the server's processing resources are fully consumed
- Establishing many simultaneous login sessions to a server so that other users cannot start login sessions
- Broadcasting on the same frequencies used by a wireless network to make the network unusable
- Consuming all available disk space by creating many large files.

For most organizations, including PCC, network bandwidth is so large that a single attacking machine cannot cause a network DoS. Instead, attackers perform distributed denial of service (DDoS) attacks, which coordinates an attack across many computers. If enough hosts are used, the total volume of generated network traffic can consume not only the resources of a targeted host but also the available bandwidth for other applications. As criminal technology has grown DDoS attacks have become an increasingly severe threat. With web servers down the lack of availability of computing and network services causes significant disruption and major financial loss. No organization is completely safe from DDoS attacks but incident response plans can help in two ways. First, knowing the attack is underway technology engineers can react and recover. Second, engineers can gather forensic information and the capability of prosecuting the attackers is very real.

Type of Attack - Reflector DoS Attacks
In a reflector attack, a host sends many requests with a spoofed source address to a service on an intermediate host. The service used is typically User Datagram Protocol (UDP) based, but can be TCP/IP as well, which makes it easier to spoof the source address successfully. Attackers often use spoofed source addresses because they hide the actual source of the attack. That host generates a reply to each request and sends these replies to the spoofed address. Because the intermediate host unwittingly performs the attack, that host is known as a reflector. During a reflector attack, a DoS could occur to the host at the spoofed address, the reflector itself, or both hosts.

Type of Attack - Amplifier Attacks
Like a reflector attack, an amplifier attack involves sending requests with a spoofed source address to an intermediate host. However, an amplifier attack does not use a single intermediate host. Instead, its goal is to use a whole network of intermediate hosts. It attempts to accomplish this action by sending an ICMP or UDP request to an expected broadcast address, hoping that many hosts will receive the broadcast and respond to it. Because the attacker's request uses a spoofed source address, the responses are all sent to the spoofed address, which may cause a DoS for that host or the host's network. Most environments block amplifier attacks by configuring border routers to not forward directed broadcasts, but some still permit them.

Type of Attack - Flood Attacks
A DDoS attack that makes a resource unavailable by initiating large numbers of incomplete connection requests is considered a flood attack. This type of attack overwhelms capacity, typically preventing new connections from being made. Flood attacks can occur using many different methods resulting in DDoS. One example is a peer-to-peer attack, which involves an attacker disconnecting a peer-to-peer file sharing hub from its peer-to-peer networks and redirecting traffic to a victim's Web site. When thousands of computers try to connect to what they think is the file sharing hub, the victim's Web server becomes overwhelmed, causing it to fail.

Another example of a flood attack is a synflood, which occurs when an attacker initiates many TCP connections in a short time by sending SYN packets but does not complete the TCP three-way handshakes necessary to fully establish each connection.

DOS and DDoS - Incident Prevention
The following items provide additional recommendations for preventing DoS incidents:

- Configure the network perimeter to deny all incoming and outgoing traffic that is not expressly permitted.
- Blocking the usage of services, such as echo.
- Performing egress and ingress filtering to block obviously spoofed packets.
- Blocking traffic from unassigned IP address ranges, known as bogon lists.
- Configuring border routers not to forward directed broadcasts.
- Limiting incoming and outgoing ICMP traffic to only the necessary types and codes.
- Blocking outgoing connections to common IRC, peer-to-peer service and instant messaging ports if the usage of such services is not permitted.

- Implement rate limiting for certain protocols, such as ICMP, so that they can only consume a designated percentage of the total bandwidth. Rate limiting can be implemented at the organization's network perimeter, border routers and firewalls.
- On Internet-accessible hosts, disable all unneeded services, and restrict the use of services that may be used in DoS attacks, configure DNS servers so they do not permit recursion.
- Ensure that networks and systems are not running near maximum capacity.

DOS and DDoS - Detection and Analysis

- DoS and DDoS attacks pose some additional challenges in terms of incident analysis:
- DoS attacks often use connectionless protocols (UDP and ICMP) or use a connection-oriented protocol in such a way that full connections are not established (e.g., sending TCP SYN packets to create a synflood attack). Therefore, it is relatively easy for attackers to use spoofed source IP addresses, making it difficult to trace the source of attacks. ISPs may be able to assist in tracing the activity, but it is often more effective to review logs for previous reconnaissance activity that appears to be related. Because the attacker would want to receive the results of the reconnaissance, such activity is unlikely to use a spoofed address, so it may indicate the location of the attacker.
- DDoS attacks often use thousands of workstations that are controlled by a single handler (or no handler at all). These workstations usually have bots installed that are considered "zombies" and are activated by the controller to attack other systems. The victim site will not see the IP of the handler, and even if it could, it is likely that it is just another host that the attacker has compromised.
- Network-based DoS attacks are difficult for IDS/IPS sensors to detect with a high degree of accuracy. For example, synflood alerts are one of the most common false positives in network IDS/IPS products. If an attacker performs a rapid SYN scan, many IDS/IPS products will report it as a synflood, even though the activity is sending only one request to each port. If a server crashes, hosts trying to reconnect to it may keep sending SYN packets. Sometimes many legitimate connections in a short time (e.g., retrieving many elements of a Web page) will also cause a synflood alert to be triggered.
- When an outage occurs, no one may realize that a DoS attack caused it. For example, a Web server may crash occasionally as a result of operating system instability, requiring a reboot for its functionality to be restored. If an attacker sends some specially crafted packets to the Web server that caused it to crash, system administrators may assume the crash resulted from the operating system's instability and not realize that an attack took place.