INCIDENCE RESPONSE

Computer *crime*:

It is defined as any criminal act during which a computer or computing device is used in the commission of a crime. The goal of computer crime can be anything that negatively impacts in some way, shape, or form the operations of a company, individual, or government.

Incident Response Policies

The IRP defines the course of action that a company or organization will take in the time following a security incident. It includes following details:

Who will determine when and if a security incident has occurred?
Which individuals and/or departments are to be notified?
The means through which they will be notified?
Who will be responsible for responding to the incident?
Appropriate response guidelines?
What you as a system administrator will be responsible for doing in the event of an incident?

who will participate in the incident response will depend on organization, assets involved, and the overall severity of the situation. The personnel involved can also determine which information can be released and to whom.

Phases of an Incident and Response

PHASE	DESCRIPTION
RESPONSE	It is important to early on establish just what has actually occurred. Is the incident an actual security incident or is it something else? The incident response team will be the ones responsible for making this determination as well as making the determination or discovery as to what was impacted
TRIAGE	The next step after the determination that a security incident has occurred is to determine how seriously the incident has impacted critical systems. Remember, not all systems or services will be affected the same way, and so some will require more attention than others. Also remember that some systems are more mission critical than others and will require more attention as well. In a computer crime security incident scenario, once the incident response team has evaluated the situation and determined the extent of the incidents, a triage approach will be implemented and the situation will be responded to according to criticality. If multiple events have occurred, the most serious event will be addressed first and remaining events will be investigated based on risk level.
INVESTIGATION	Once the response team discovers the cause of the problem, the investigative process can start. The investigation is designed to methodically collect evidence without destroying or altering it in any way. This process can be performed by internal personnel or by an external team where appropriate. The key point in either case is that the team involved in the investigative process understands how to collect the evidence properly because the end result of the process may be to take this collected information to court. So who may investigate a security incident may vary depending on the extent and type of security breach. In some cases, internal teams or consultants may be all that's needed to investigate and analyze a crime scene; however, in some cases that may not be enough. It is possible under certain conditions to get local law

	enforcement involved in the investigation of a crime. This option will vary depending on the skills that the local law enforcement have. Some police departments are adept at dealing with computer crime, but this is not always the case. Investigations should never be taken lightly, and once local law enforcement is involved other issues arise. Police departments may not be able to respond in a timely fashion because corporate security problems are not part of the police mission and therefore are low priority.
CONTAINMENT	It is necessary early on in the process of incident response to contain and control the crime scene as much as possible. When considering a crime scene it is important that no alterations or tampering of any sort occur to avoid damaging of evidence. This means that the crime scene should not be tampered with in any way including disconnecting any devices, wires, or peripherals or even shutting down the system. It is important to let trained professionals do their job at the crime scene.
ANALYSIS AND TRACKING	Evidence that has been gathered is useless unless it is examined and dissected to determine what has occurred. At this point the company will either be involving external professionals to examine the evidence or employing its own internal teams. These teams will be responsible for determining what evidence is relevant to the investigation and what is not. Additionally the team must maintain the chain of custody, which means that evidence must be accounted for and under positive control of the team at all times.
RECOVERY	During the recovery phase it is assumed that all relevant evidence has been collected and the crime scene has been cleaned. At this point the crime scene investigation has been completed and the effected systems can be restored and returned to service. This process will include restoring and rebuilding operating systems with their applications and data from backups or drive images.
REPAIR	In the event that a system has experienced substantial damage in the course of an attack, it becomes necessary to repair the system. The recovery process is designed to deal with rebuilding a system after evidence has been collected, but it does not account for potential damage done that may need to be repaired. Also, the collection of evidence may have required the removal of components to preserve the evidence, and those components will need to be replaced.
DEBREIFING AND FEEDBACK	When the situation is under control, you will need to debrief and obtain feedback from all involved. The incident happened for a reason; presumably at this point you have determined what this reason is, at least in some part. The goal of this phase is to determine what the company did right, what it did wrong, and how to improve. Additionally, depending on the crime it may be necessary to start the process of informing clients and other agencies and regulatory bodies of the breach. This last point may be the most important one because failure to inform the appropriate regulatory bodies can mean you or your company is guilty of a crime

Incident Response Team

As organizations grow in size and importance it is likely that they will build or already have a group known as an incident response team. it includes people who can properly collect and preserve the evidences of a crime. The goal of security response is to have a team in place that is well versed and aware of how to deal with security incidents. The goal of security response is to have a team in place that is well versed and aware of how to deal with security incidents. These members will know what to do and have been drilled on how to do it in the event an incident occurs. An IR team may include following memebers IT personnel, Human resources, Public relations, Local law enforcement, Security officers, Chief security office.

Incident Response Plans

The plan will include all the steps and details required to investigate the crime as necessary. Some of the elements required to investigate a security crime are the following:

1> If an IRP exists and is relevant, follow the process outlined in this plan.
2> If an IRP does not currently exist, is out of data, or is irrelevant, then designate a lead examiner for the process so there is a coordinated response.
3> Examine and evaluate the nature of the events that occurred and, as much as possible, determine the damage that has been incurred by the systems, services, and other items involved.
4> Document and identify all involved components of the incident as completely as possible. Undertake a complete analysis to determine the different risk priorities for all systems, services, and other processes involved.
5> Evaluate the need for outside expertise or consultants. Determine if local law enforcement involvement is needed.
6> Determine how to contain the crime scene, including hardware, software, and other artifacts present. Decide how to collect the required evidence at the crime scene with special provisions for electronic evidence, hardware, and other items.
7> Set up a procedure for interviewing personnel who may have additional knowledge or other information to share that would be beneficial to investigating the crime scene.
8> Put in place a reporting mechanism for the crime and determine who should receive the report, such as regulatory bodies.

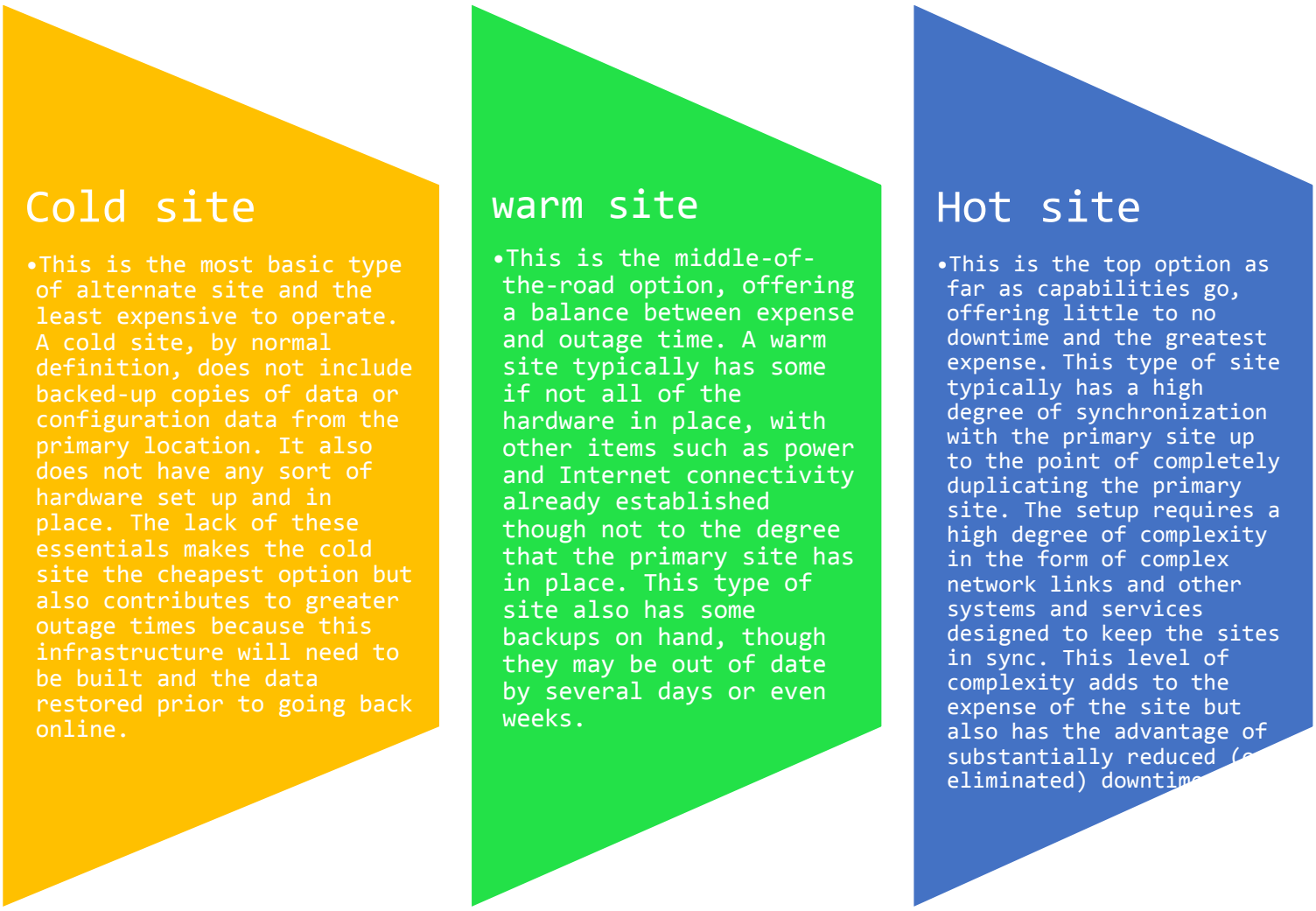
Business Continuity Plan

This policy defines how the organization will maintain what is acceptable as normal day-to-day business in the event of a security incident or other event disruptive to the business. This plan will be called into play in the event that a disaster or severely disruptive event occurs and causes the business to become unavailable. If a company provides services to customers or clients and the business becomes unavailable, the company loses both money and the faith of its customers—something that no business wants to experience. A BCP is designed to ensure that vital systems, services, and documents that support the business remain available to alert key stakeholders and recover assets even when the bulk of critical systems are down. After BSP comes disaster recovery plan(DRP), The DRP typically will include a list of responsible individuals who will be involved in the recovery process, an inventory of vital hardware and software, steps to respond to and address the outage, and how to rebuild affected systems.

Supporting Business Continuity and Disaster Recovery

Several techniques can be used to keep the organization running and diminish the impact of a disaster when it occurs. **Fault tolerance** is a valuable tool in the company arsenal because it provides the ability to weather potential failures while providing some measure of service. While this service may not be optimal, it should be enough to maintain some business operations even if not at the normal level of performance. Fault-tolerant mechanisms include service and infrastructure duplication designed to handle a component failure when it occurs. Another mechanism commonly used by companies is **high-availability architecture** High availability can be attained by having redundant systems and reliable backup systems. When implemented properly, it means that the services you rely on to do your job and provide service to clients are available and ready to use for the greatest possible amount of time. We expect that the system should be available 100% of the time which is not possible in very long hours of operation. A document that is commonly mentioned when discussing high availability and fault tolerance is a **service-level agreement (SLA)**. This document spells out the obligations of the service provider to you, the client. Specifically, an SLA is a legal contract that lays out what the service provider will provide, at what performance level, and steps that will be taken in the event of an outage. This document can include specific performance and availability levels that are expected and the associated penalties for not meeting these levels. Additionally it will spell out the parties responsible and the extent of their responsibilities in the event of a disaster, such as who will take care of the problems related to the disaster.

Alternate sites are another technique used in the event of a system failure or disaster. The idea is to have another location to conduct business operations from in the event of a disaster. Under ideal conditions all operations will be moved to an alternate site if the primary or normal site is no longer able to provide services. There are 3 types of A.S. :→



Before an alternate site can work, however, the company must have a data backup, and this backup must be kept secure because it contains information about the company, its clients, and its infrastructure. Backups should be stored safely and securely, with copies kept both onsite and offsite to give optimal protection. Mostly we should encrypt these backups to avoid unwanted disclosure if stolen. Other safeguards should be taken to protect the backups from **environmental concerns** such as **fire**, **floods**, and **earthquakes**, to name a few.

Planning for Disaster and Recovery

In order to properly plan for disaster recovery you will need to know where you stand, specifically where the company stands.

In order to properly plan for disaster recovery, you should observe the following guidelines and best practices:

1>Once your organization has established a BCP it is important for this **plan to undergo regular testing and review.** Consider conducting simulations and drills designed to evaluate the efficacy of the plan.

2>If the company has not recently tested the DRP, make it a point to do so. Much like BCPs, consider the **use of drills and other similar types of simulations to evaluate how well the DRP functions.**

3>Always consider and evaluate the proper redundancy measures for all critical resources. Look for **adequate protection for systems such as servers, routers, and**

other devices in the event they are needed for emergency use.

4> Check with all critical service providers to ensure that they've taken adequate precautions to guarantee that the services provided will be available.

5> Check for the existence or the **ability to obtain spare hardware wherever necessary.** Ensure that the devices are not only appropriate for use but also can be obtained quickly in an emergency.

6>Evaluate any existing SLAs currently in place so that you know what constitutes acceptable downtime.

7>**Establish mechanisms for communication that do not require the company resources,** which may be unavailable. Such communication channels should also take into account that power may be unavailable.

8>**Ensure that the organization's designated hot site can be brought online immediately.**
9>**Identify and document any and all points of failure,** as well as any up-to-date redundancy measures that have been put in place to safeguard these points.

10>**Ensure that the company's redundant storage is secure.**

Evidence-Collection Techniques

Proper collection of evidence is essential. when a crime has been suspected it becomes mandatory to have trained professionals involved in the process. If this is not you, then you should not disturb the crime scene; rather you should contact a manager or someone in charge for guidance on how to proceed. Only the trained professional should do the evidence collection as the novice can inadvertently damage the evidence.

Types OF Evidence

Evidence	Description
Best	The best evidence is category evidence that is admissible by requirement in any court of law. The existence of best evidence eliminates your ability to use any copies of the same evidence in court.
Secondary	Secondary evidence is a copy of the original evidence. This could be items such as backups and drive images. This type of evidence may not always be admissible in a court of law and is not admissible if best evidence of the item exists.
Direct	Direct evidence is received as the result of testimony or interview of an individual. This individual could have obtained their evidence as a result of observation. Evidence in this category can be used to prove a case based on its existence.
Conclusive	Conclusive evidence includes that which is above dispute. Conclusive evidence is considered so strong that it directly overrides all other evidence types by its existence.
Opinion	Opinion evidence is derived from an individual's gut feelings. Opinion evidence is divided into the following types: Expert–Any evidence that is based on known facts, experience, and an expert's knowledge. Non- expert–Any evidence that is derived from fact alone and comes from a non-expert in the field.
Corroborative	Corroborative evidence is obtained from multiple sources and is supportive in nature. This type of evidence cannot stand on its own and is used to bolster the strength of other evidence.
Circumstantial	Circumstantial evidence can be obtained from multiple sources, but unlike corroborative evidence it is only able to indirectly infer a crime.

Chain of Custody

When collecting evidence the chain of custody must be maintained at all times. The chain of custody documents the whereabouts of the evidence from the point of collection to the time it is presented in court and then when it is returned to its owner or destroyed. A chain of custody needs to include every detail about the evidence, from how it was collected up to how it was processed. A chain of custody can be thought of as enforcing or maintaining six key points. These points will ensure that you focus on how information is handled at every step:

What evidence has been collected?

How was the evidence obtained?

When was the evidence collected?

Who has handled the evidence?

What reason did each person have for handling the evidence?

Where has the evidence traveled and where was this evidence ultimately stored?

if you are involved to keep the chain of custody information up to date at all times. Every time any evidence is handled by an investigator, you must update the record to reflect this. You may be asked at some point to sign off on where evidence was or that it was collected from you.

Rules of Evidence

presented in court unless certain rules are followed, and you should review those rules ahead of time. The five rules of evidence presented here are general guidelines and are not consistent across jurisdictions:

Reliable—The evidence presented is consistent and leads to a common conclusion.

Preserved—Chain of custody comes into play and the records help identify and prove the preservation of the evidence in question.

Relevant—The evidence directly relates to the case being tried. Properly identified—Records can provide proper proof of preservation and identification of the evidence.

Legally permissible—The evidence is deemed by the judge to fit the rules of evidence for the court and case at hand.

Recovering from a Security Incident

When a security incident happens, and it will happen, the company should have a plan to restore business operations as quickly and effectively as possible. This may require you and possibly your team to correctly assess the damage, complete the investigation, and then initiate the recovery process. From the time of the initial security incident onward, the organization presumably has been operating at some reduced capacity, and so you need to recover the systems and environment as quickly as possible to restore normal business operations. Other key requirements are the need to generate a report on what happened and the ability to communicate with appropriate team members.

Reporting a Security Incident

Once an incident has been responded to and a team has gotten involved to assess the damage and start the cleanup, the required parties will need to be informed. These parties will be responsible for getting the ball rolling whether it is legal action, an investigative process, or other requirements as necessary. When considering how to report a security incident the following guidelines are worth keeping in mind and can prove helpful at the time of crisis:

1>Adhere to known best practices and guidelines that have been previously established. These best practices and guidelines will describe how to best assess the damage and implement loss control as necessary.

2>Wherever feasible refer to previously established guidelines as documented and described in the company IRP. The IRP should include guidelines on how to create a report and who to report to. Furthermore, the IRP should define the formats and guidelines for putting the

report together in order to ensure that the information is actually usable by its intended audience.
3>Consider the situations where it is necessary to report the incident to local law enforcement in addition to the company officials.
4>Consider the situations and conditions about when and if the security incident must be reported to regulatory bodies as required by law.
5>In situations where security incidents are reported outside the organization, note this in the company incident report.

During the preparation of a security incident report include all the relevant information to detail and describe the incident. The following items should be included at a minimum:
A timeline of the events of the security incident that includes any and all actions taken during the process.
A risk assessment that includes extensive details of the state of the system before and after the security incident occurred.
A detailed list of any and all who took part in the discovery, assessment, and final resolution (if this has occurred) of the security incident. It is important to include every person who took part in this process regardless of how important or unimportant their role may be perceived.
Detailed listing of the motivations for the decisions that were made during the process. Document these actions in a format that states what each action was and what factors led to the decision to take the designated action.
Recommendation as to what could be done to prevent a repeat of the incident and what could be done to reduce any damage that may result.
Two sections in the report to ensure that it is usable by all parties. First, prepare a long-format report that includes specific details and actions that occurred during the security incident. Second, include an executive-level summary that provides a high- level, short-format description of what occurred.
All evidence, no matter the type, may not be admissible in court. Evidence cannot be