	PALACIOS POLICE DEPARTMENT
	Policy 9.2 Computer Security and Incident Response
	Effective Date:1/04/2021 | **Replaces:2/07/2006**
	Approved: Milton Rivera **Milton Rivera,Chief of Police**

BACKGROUND

Computer security events happen on a regular basis and organizations must be prepared to respond in a timely and appropriate fashion. The intent of this document is not to proscribe a specific set of responses but rather to outline the process associated with responding. While a number of the steps will be presented in a linear fashion there may be opportunities to conduct steps in parallel. There are also a number of administrative and managerial issues that need to be considered separate and apart from the actual technical response.

1. INITIAL RESPONSE

a. The principle objective of this incident response plan is to ensure business continuity and to support disaster recovery efforts. The scope and nature of any response must be consistent with the fundamental objectives of the business.

b. As with any crisis, the initial response to a computer security event involves a rapid assessment of the situation and the execution of a number of "immediate action" steps designed to contain the problem and limit further damage.

i. Upon detection of a suspected security event, notifications should be made to the Chain of Command immediately. IT should be notified immediately to assess the situation and direct the initial response

ii. Two issues that shall be addressed immediately. First, is the compromised system an immediate threat to external resources or critical internal resources, and second, are malicious processes running which could result in a substantial loss of data on the compromised system? Systems that pose an immediate threat to external entities or critical business functions shall be isolated from the network. Depending on the network architecture and available resources, this may mean physical isolation (i.e., removal of an Ethernet cable or phone line) or logical isolation, through the use of firewalls and routers. If a malicious process that could result in substantial loss of data appears to be running on the compromised system, the system should be immediately disconnected from the power source. In routine situations, the decisions to isolate and power down the potentially compromised system shall be made as part of the investigative process. Systems supporting life-support or mission critical functions should only be disconnected only after careful consideration of the risks and under the direction of the Information Services Director. Once the initial decision to isolate and/or unplug the device has been made, a more calculated analysis of the problem can take place.

2. INVESTIGATIVE PROCESS

- a. The first issue that shall be resolved is determining the nature of the event. Where possible, non-malicious causes (i.e., software configuration errors and hardware failures) should be investigated and ruled out. Events determined to be non-malicious in nature should be documented and resolved in accordance with organizational policies. Where an obvious non-malicious cause cannot be identified, the incident should be responded to as a hostile event.
- b. If a decision has been made to respond to the issue as a hostile event, the nature and intent of that response needs to be defined. If there is no desire to collect data for its intelligence or law enforcement value the incident can be responded to in much the same way as a non-malicious event. Since the extent and mechanics of the compromise will never be fully understood any system returned to service must be appropriately rebuilt, patched, and hardened before being connected to the network.

c. Regardless of the organizational objectives (immediate return to service vs. investigation) some amount of initial data collection/preservation shall be undertaken. Because the extent of the compromise is not known, this phase should be as non-alerting as possible. The following are recommended steps to include:

i. Review and analysis of the initial indicators of compromise

ii. Inventory of operating system and applications/services (version and patch level)

iii. Preserve and review system/application logs (copy to secure offline media)

iv. Preserve and review security device logs (copy to secure offline media)

v. Non-confrontational interviews of system administrators and users (as indicated)

vi. Examination of other hosts on the network segment or hosts that share a trust relationship

vii. Organizations not engaging in a full investigation may be able to infer the factors that led to a compromise from the limited data collected during this phase of the response. Organizations engaging in an investigation will use this data along with data collected during subsequent steps to develop an understanding of the vulnerability, exploit, and actions of the intruder.

d. Once the decision has been made to investigate an event, the Information Services Director shall address a series of questions that will influence both the nature and the cost of the investigation.

i. The fundamental issues that need to be addressed include referring the matter to law enforcement (this issue should be considered at the outset and periodically during the course of an internal investigation), conducting the investigation with in-house resources, contracting the task out, or working collaboratively.

ii. The issue of responding immediately vs. monitoring the situation to develop additional information about the intruders, their methodologies and objectives must also be resolved. Before making a decision regarding any of these issues investigators should consult with Information Services Director and City Management.

iii. If criminal activity is suspected, the Chief will assign CID. Typically, events which result in significant financial loss (as measured by both opportunity costs and recovery costs), loss of life or potential loss of life, attacks on critical infrastructure, or have the potential to cause widespread loss should be presented to law enforcement. As with any criminal matter, the threshold on law enforcement involvement will vary by jurisdiction. Once law enforcement joins the investigation, they have the discretion to dictate both the pace and objectives of the investigation.

iv. If a matter is being investigated internally, the Chief and City Manager shall make a decision on whether to use in-house or contract investigative resources.

e. Determination to Restore or Monitor

i. IT shall at the outset of an investigation determine whether to immediately restore the system to a secure and operational state or monitor the system in an attempt to collect additional information on the scope and nature of the compromise.

ii. Once the decision has been made to monitor a system, safeguards shall be implemented that allow for rapid response should the compromised system begin attacking external or critical internal resources or should a malicious process be activated that attempts to destroy valuable data on the system.

1. Monitoring tools should be tuned to alarm on suspicious outbound traffic and someone should be tasked with immediately disconnecting the system from the network and/or power source if instructed to do so by the investigating team.
2. The actual mechanics of monitoring will vary by network but will invariably involve the use of a network sniffer and possibly an intrusion detection device.
3. The typical objectives of monitoring a compromised system include identifying the source(s) of the intrusion, determining the mechanics of the compromise, identifying the goals/objectives of the intruder, and defining the true scope of the problem.
4. In the course of monitoring hostile activity, additional compromised systems, to include systems external to the organization may be identified. The Information Services Director shall decide how and when to apprise those external organizations of the potential compromise. External notifications should only be made after coordination with organizational advisors to include City Attorney, City Manager and Chief.

iii. An assessment of the compromised system will be conducted. The specific tools and techniques will vary by operating system and event but the basic intent is constant; collect and analyze both volatile and non-volatile information from the system.

Volatile data must be collected from the system prior to powering the device down. The volatile information of greatest interest includes a memory dump, a listing of active processes/applications and their associated network ports, active connections, and current users. The processes used to collect the data should be adequately documented and the data itself written to secure removable media (i.e., a floppy) or to an off-host (networked) resource. The investigator shall assume that all applications on the system being examined have been compromised and cannot be trusted to return accurate information. Examiners should provide their own trusted tools that can be either run locally (statically compiled binaries run from removable media) or over the network.

f. Handling Digital Evidence.

i. Using the proper tools, an unlimited number of identical copies of an item of digital evidence shall be created for use by the examiner.

ii. The process of creating an evidentiary copy involves “bit level duplication”. The resources, experiences, and preferences of the examiner will dictate which tools are utilized.

iii. Critical to the process of creating an identical copy or “image” of a drive is ensuring that the original is not altered by the procedure and that each bit has been accurately recorded on the copy. Mounting the drive to be imaged as a “read-only” device can satisfy the first requirement while hashing algorithms such as MD5, which create a “fingerprint” unique to the input source, can be used to validate the copy process. The characteristics of the MD5 hashing algorithm are such that the alteration of a single bit in a file of any size will result in a different fingerprint. MD5 can be used to verify that the item of original digital evidence and any instances of Duplicate Digital Evidence (DDE) are identical.

iv. Whenever possible, the original item of evidence should be retained and used to generate a first generation DDE copy which is in turn used to generate all subsequent DDE copies. If the original evidence (i.e., production hard drive) cannot be retained as evidence, a first generation copy should be made and treated in the same manner as an item of original evidence would be. Forensic examinations should be conducted on subsequent generations of DDE.

v. Once the volatile information has been collected, a decision shall be made by the Information Services Director whether to shut down the system and “image” the drives or, to attempt to image the “live” system. For mission critical systems that cannot be taken off line, the system will have to be imaged while in operation, potentially over a networked connection. In situations where the system can be taken offline, the original drives should be retained as evidence whenever possible. If the original drives cannot be retained the reasons should be documented. The actual process of creating a forensically sound copy will vary by tool and situation. Examiners unfamiliar with their chosen application should consult the documentation prior to attempting to image a drive or live file system. Once taken as evidence, access to the original drives, or 1st generation evidentiary copy, should be

restricted. Any access to or transfer of custody over the physical article should be documented on a chain of custody form.

g. Data Analysis

i. Once a suitable copy of DDE is available for examination, the analyst can use any number of commercial or open source tools to conduct the analysis. The analytical process should be thoroughly documented, to ensure defensible/repeatable results. The specifics of an examination will vary by incident but in general, an analyst will look for evidence of contraband files, unauthorized access to intellectual property, logs/indicators of hostile acts directed at or originating from the compromised host, and indicators of specific compromised resources (files, user accounts, and other systems).

ii. If during the course of the examination evidence surfaces that indicates trust relationships were exploited the scope of the investigation may have to be expanded. If it becomes apparent the security of other organizations was compromised Information Services Director, City Manager, and Communications Coordinator shall decide on the timing and nature of any notification.

3. RECOVERY

a. Once the volatile data has been captured and a forensically sound copy of the compromised device secured, work can begin on retuning the system to service. Because the true scope of a compromise often remains in doubt the most prudent course of action is usually to rebuild the system from trusted media. Data should be restored from a trusted source and validated before being relied upon. The operating system and all applications should be updated wherever possible, patched, and all unnecessary services disabled. All system passwords shall be changed and hosts with which the compromised system shared a trust relation examined for possible signs of compromise. If the root cause for the compromise has been determined, appropriate steps should be implemented to mitigate the risks.