Agency Incident Response Guidelines

Commonwealth of Kentucky

Commonwealth Office of Technology

Effective Date: 01/01/2015
Revision Date: 03/12/2018
Reviewed Date: 03/12/2018
Reviewed Date: 08/23/2023

Table of Contents

1 INTRODUCTION

The Commonwealth of Kentucky, Commonwealth Office of Technology (COT), Office of the Chief Information Security Officer (CISO) is responsible for the efficiency and effectiveness of IT security functions and responsibilities across the Commonwealth. As part of this responsibility, the CISO established the following Agency Incident Response Guidelines to prepare for and react to threats to the Commonwealth's network and information systems at the agency level.

OBJECTIVE

This plan is a template that agencies can use to create a security event/incident evaluation and response process. The objective of the Agency Incident Response Guidelines is to outline the steps to take when a security incident has occurred. The Agency Plan also aims to lessen the costs of disruption to the Commonwealth's services and assets, whether they are monetary, such as those associated with replacing damaged equipment or infrastructure, or whether they be costs associated with the loss of business data or a loss to the Commonwealth's reputation.

1.1 *OVERVIEW*

COT categorizes the steps involved in handling a security incident into five phases:

Phase 1 – Notification, Assessment, and Initial Response
Phase 2 - Containment
Phase 3 - Eradication
Phase 4 - Remediation

Phase 5 - Post-incident Activities and Lessons Learned

The actions taken in some of these phases are common to all types of security incidents, regardless of the type of event or events. It is important to prioritize incidents; sometimes an incident may be so complex that it is impossible to do everything at once. To respond to it, priorities are essential. As a rule, the priorities for Kentucky COT incident response are:

Priority 1:	Protect human life and safety.
Priority 2:	Protect confidential and/or sensitive data and information, particularly as mandated by state or federal laws.
Priority 3:	Protect other data and information, including proprietary, scientific, managerial, and other data and IT applications.
Priority 4:	Prevent damage to systems (e.g., loss or alteration of system files).
Priority 5:	Minimize disruption of computing resources.

Once incident responders address personnel safety and security, it is generally more important to save data than system software and hardware. Another important concern is the effect on others, beyond the systems and networks where the incident occurs. Within the limits imposed by government regulations, it is always important to inform affected agencies as soon as possible. Moreover, responders must use forensically sound procedures whenever possible in order to assist in containment, eradication, and recovery activities, in addition to aiding in potential prosecution of identified perpetrators for successful or failed attacks.

1.2 *DEFINITION*

For the purposes of incident response, there is a difference between "events" and "incidents". A security "event" is an observable occurrence in a system, network, or daily operation. Events themselves are not necessarily adverse. Non-adverse events typically fall into, but are not limited to, the following types of activities:

- Receiving SPAM e-mail
- E-mail indicating virus was removed from a mail or relay server
- E-mail hoaxes, solicitations, or chain letters
- Elevated scan attempts that do not significantly degrade resources

Incidents are adverse events. According to the United States Computer Emergency Readiness Team (US-CERT), an incident is the act of violating an explicit or implied security policy. Examples of these types of activities are:

- Attempts (either failed or successful) to gain unauthorized access to a system or its data
- Data breaches of highly regulated and controlled data such as Payment Card Industry (PCI), Personally Identifiable Information (PII), Health Insurance Portability and Accountability Act (HIPAA), or other federal or sensitive information
- Unwanted disruption or denial of service
- Unauthorized use of a system for the processing or storage of data
- Receiving a threatening e-mail or phone call
- Inappropriate or illegal use of an system or resource in violation of policy
- Successful spear-fishing e-mails targeting specific organizations or areas

When attempting to determine if an activity or event qualifies as an incident, the following guidelines can help establish if an incident occurred:

- There is a risk to data integrity
- There is a risk to availability of a resource

- There is a risk to confidentiality of data
- There is a violation of a policy or statute

The agency will need to create a process internally to evaluate incidents and determine if the agency should handle the event internally or report the findings to the COT Office of the CISO according to the Commonwealth's Policy CIO-090 (Incident Response Policy).

2 COT and AGENCY ROLES AND RESPONSIBILITIES

2.1 *COT*

If an agency submits a security event to COT for investigation, COT will evaluate the information and determine whether to initiate the incident response process. The Chief Information Officer (CIO) or CISO will decide to initiate the incident handling response and assign a coordinator for that response. While each incident will require tailored responses, general roles and responsibilities will be similar for each incident. The CIO or CISO will assign a Security Incident Response Coordinator (SIRC) who will be responsible for managing all incident response personnel, activities, incident forensics, and documentation. The CIO or CISO, and the SIRC may also identify and alert various teams.

2.2 *AGENCY*

Any agency involved with security incidents will need to address the security threat, in coordination with COT. The agency should have a documented process outlining how to identify and classify events and incidents, internal response coordination, and coordination with COT and other agencies as necessary. This document can serve as a template for creating the process.
The agency may also assign a point person to act as the contact for their agency. Each affected agency may also have a manager and/or executive assigned to the oversight teams (Executive and Management CERTs as described later in this document).

COT and agency personnel will be part of an incident handling team that will provide a coordinated response to security incidents throughout the organization and agencies. Many people may be involved during the response to an active security incident. Notably, the COT response plan will address the technical and security aspects of incident response. The agencies will be responsible for addressing the business aspect of incident response.

As the situation warrants, the CIO or CISO—working with the Security Incident Response Coordinator—may decide to activate various response teams. These teams will usually include the Executive Cyber Emergency Response Team (E-CERT), and Subject Matter Expert (SME) teams. For incidents that may require more involvement by Directors and Branch Managers, the E-CERT may also create a Management CERT (M-CERT) to coordinate responders and provide support. Certain security compromises may require additional professional personnel, including Public Information Officers (PIO) and Offices of General Counsel (OGC). It will be important for agency to have their PIO and General Counsel, Executive Management involved as they determine steps to take. If this has been sent to COT then they should work together in determining next steps.

2.3 *Public Information Officer (PIO)*

The CISO and agency may need to publicize security incidents and recovery information. This need may result from a state or federal law or policy, or a specific incident becomes so prevalent or serious that the response team feels it necessary to disseminate information widely and quickly. When information must be disclosed to the public, the agency or COT should coordinate with the Public Information Officers for the Finance Cabinet and the affected agencies. Moreover, circumstances may dictate close coordination with the Governor's Office to ensure an appropriate statewide response and accurate, consistent information dissemination.

The announcements/dissemination of information must adhere to state and federal law requirements; however, when possible, it is best to release as little detail as possible if there is a type of attack and remediation efforts before the investigation is complete. The CISO and Public Information Officers should work closely with the Office of General Counsel to ensure compliance with information release laws when incident circumstances compel a public response.

2.4 *Office of the General Counsel (OGC)*

When security incidents warrant, the CISO or Agency may need to consult with various Offices of General Counsel. Some incidents may involve federal tax data, health information, personal identifiable information, or other sensitive information. OGCs can help navigate any complex legal issues and identify appropriate reporting responsibilities. Furthermore, COT may require legal advice concerning culpability and compliance issues. It is not possible to identify all situations in which responders should seek legal advice, but the CISO and response teams should keep OGCs involved for severe or widespread security incidents. When in doubt, it is good policy to apprise OGC of potential issues related to incident response.

2.5 *Agency Level Incident Response Team*

The Agency Level Incident Response Team is the focal point for all security incidents within the agency. This team can include management, SMEs, etc. The mission of the Agency Level Incident Response Team is to:

- Assist in protecting the agency systems and business, and the data they contain, from the effects of security incidents;
- Provide a central point of contact for the reporting and dissemination of information about security incidents;
- Coordinate the activities of other personnel in the investigation of, response to, and recovery from security incidents;
- Minimize any negative impact of an agency security incident on business operations and public image;
- Minimize disruption to both internal and external customers;
- Collect necessary data and evidence for prosecution; and
- Ensure activities and actions are consistent with the Incident Response priorities.

3 COMMUNICATIONS AND NOTIFICATION PROCEDURES

As early in the incident handling response as possible, COT and/or the Agency should establish communications protocols for addressing the incident. This will include determining who to contact and what information may be divulged to other entities. The Agency must determine what information to relate to others and must emphasize what NOT to reveal (e.g. incident response techniques, software compromised or used, etc.) Ideally, all members of the response teams should have this communications information with them during their work. In addition, when possible, the Agency should coordinate with the Office of General Counsel and the Public Information Office to address the communications protocols. Some of the entities that the agency must consider for contact can include the following:

- Customers
- Constituents
- System owners
- Disaster Recovery personnel
- Cabinet and Governor's offices
- Human resources

- Facilities management
- Vendors
- Law enforcement agencies (FBI, state, local, county, agency OIGs)
- Internet Service Providers
- Other state, local, and/or federal agencies
- Any other agency that may be affected by the incident

During incident handling, the team may need to provide updates to certain parties, even in some cases the entire organization. The team should plan and prepare several communication methods, including out-of-band methods (e.g., in person or paper), and select the methods that are appropriate for a particular incident. Examples of notifications should be drafted as soon as possible so that an approved notification is ready when it is first needed. Possible communication methods include:

- Email
- Paper (e.g., posting notices on bulletin boards and doors and/or distributing handouts at all entrances)
- Websites (e.g., COT Intranet or a special incident response SharePoint site)
- Telephone calls
- In person (e.g., daily briefings)
- Voice mailbox greeting (e.g., setting up a special voice mailbox for incident updates, with the greeting reflecting the current incident status)

See Appendix for sample press release and notifications.
NOTE: Electronic Information Exchange Partners (EIEP)

If EIEP experiences or suspects a breach or loss of PII or a security incident which includes SSA-provided data, they must notify the United States Computer Emergency Readiness Team (US-CERT) within one hour of discovering the incident. The EIEP must also notify the SSA Systems Security contact named in the agreement. If within 1 hour the EIEP has been unable to make contact with that person, the EIEP must call SSA‟s National Network Service Center (NNSC) toll free at 877-697-4889 (select “Security and PII Reporting” from the options list). The EIEP will provide updates as they become available to SSA contact, as appropriate. Refer to the worksheet provided in the agreement to facilitate gathering and organizing information about an incident.

4 INCIDENT HANDLING PREPRATION AND DETECTION

Agencies should be prepared to respond to security incidents quickly. This should include periodic awareness training to recognize incidents and explain reporting procedures. Users should recognize that threats could come from many directions, such as Internet, e-mail, removable media, physical theft, etc. Agencies should participate in annual training/testing (such as tabletop exercises) as part of their preparation responsibilities.

Other preparation techniques to prevent or limit incidents such as attacks and damage can include implementing sound, industry-recognized security controls; regular auditing; log management and review; software patching; and other security preventative measures.

Agencies should also be prepared for incident response by:

- Maintaining up-to-date contact information for management, security, and key response team members
- Maintaining reporting and request mechanisms for agencies, especially automated systems such as the Commonwealth Service Desk

Once an agency identifies an incident and begins their incident handling response process, the teams will begin their containment, eradication, and recovery steps (covered later in this plan).

Security Incident Reporting

Once a user, agency, COT, or other entity recognizes an incident, COT policy dictates that the user or agency should immediately contact the Commonwealth Service Desk to report the incident, severity, and other relevant information. The Service Desk will then generate an automatic help desk ticket to assign to the Security Office. The Service Desk will also maintain up-to-date contact information for security personnel for use after typical business hours. The Service Desk ticket will be the trigger for COT's response to an incident and COT will use the ticket to document the response. COT responders must recognize that not all information can be kept in the service ticket, for security reasons, as others throughout the organization will also have access to that information. COT Security Office may also initiate a security incident and will use appropriate notification procedures. If the incident is sensitive, the user or agency may contact the Security Office directly.

4.1 *PHASE 1: NOTIFICATION, ASSESSMENT, and INITIAL RESPONSE*

Each agency should create a procedure to evaluate and respond to incidents. On those occasions when the security event warrants notifying the COT Office of the CISO, the agency must report the potential incident to the Commonwealth Service Desk immediately via telephone or e-mail so that the Service Desk may contact the Security Office. Agencies also have the option of contacting the Security office directly, especially if the agency and Security office need to discuss sensitive data to provide a clearer picture of the incident.

After the agency notifies the Service Desk, the Service Desk will contact the Security Office according to established procedures. Once security personnel receive the necessary information about the incident, they must conduct a preliminary analysis and recommendation to the CISO (or CIO) on whether to classify the event as an incident and its recommended severity. At this point, the CISO or CIO must decide whether to proceed with the incident and the initial direction the investigation will take. **Only the CIO or CISO can declare any event an incident and to activate the emergency response teams.** (Of note, the CISO may designate someone to act on the CISO's behalf for event evaluation and incident declaration; this section will only reference the CISO for ease of readability.)

The CISO will appoint a SIRC to spearhead the investigation and remediation activities and will evaluate some of these factors to determine how to respond:

- Type of Incident
- If potential attack: the type, pervasiveness/scope and severity/maliciousness of attack
- Agencies affected
- COT/agency level of expertise
- Time constraints
- Monetary costs
- Loss of reputation potential
- Known defensive capabilities or weaknesses at COT or agencies
- Level of involvement required by forensics investigators

Once the CISO has gathered as much relevant information, he/she must determine the course of action. The CISO may decide that COT:

- Will not respond to the event/incident

- Will participate in an advisory role to the affected agency or agencies or act as a partner in addressing the incident
- Lead the Incident Response activities

The CISO may also modify the COT response when circumstances require. For example, if notified of an isolated attack at an agency, the CISO may elect not to activate the Incident Response Plan. However, if the CISO determines that the agency is not responding in a timely or effective manner, or the attack spreads, the CISO can declare that COT will become involved and collaborate with the agency or take over the response and investigation.

For security incidents that include or may include breaches of PII, COT and agencies must adhere to KRS 61.931-61.934 effective 1 January 2015. This statute requires COT, governmental agencies, or non-affiliated third parties that maintain or possess personal information to have reasonable security procedures and practices to protect the information. Moreover, COT, the agencies, and third parties must follow strict procedures included in the associated statutes for notification and reporting of the known or suspected PII data breaches.

4.1.1 Data Breach Requirements

While COT and agencies need to be prepared to respond to many different types of security incidents, data breaches have unique requirements related to incident response that must be addressed. The Commonwealth stores and transmits data with many different reporting requirements, to include HIPAA, CJIS, SSA, and IRS requirements among others. Depending on the type of data and disclosure or breach of that data, different agencies will have different reporting requirements to state and federal agencies as well as reporting to citizens whose data may have been breached. For more guidance on data breach notifications, please see Appendix – Data Breach Overview and Links.

4.2 *PHASE 2: CONTAINMENT PHASE*

As soon as possible after an incident is reported, the agency must begin the containment phase of incident response. The goal of containment is to limit the extent of the incident or attack and prevent the inundation of resources or broadening the damage, with an emphasis on maintaining or restoring business continuity. An attack is contained when no more harm is possible and the teams' focus pivots to the remediation phase. The containment phase may focus on both short-term and long-term containment. The short-term containment involves stopping the attack; the long-term containment includes making necessary changes to production systems to prevent repeat attacks.

It is imperative that the agency responders maintain a calm, measured approach to containment. Responders need to use proper decision-making techniques to ensure no further damage is created by ill-advised activity. Many of COT's guidelines in the containment phase are highlighted in NIST document 800-61 (Revision 2), **Computer Security Incident Handling Guide.**

Requirements and considerations during the Containment Phase include:

- Document all steps
- Conduct a risk assessment of the incident
- Depending on the focus, teams should consider:
    - Shutting down affected systems ○ Disconnecting systems from the network ○ Disabling the network ○ Disabling services such as FTP, telnet, e-mail, or any other service that may be affected or may propagate the attack
    - Stopping the attack from more damage by shutting off the power, pulling network cables, or blocking ports
    - Isolating affected systems from other resources.

- Conducting forensics and evidence preservation (e.g., memory dumps, drive images) ○ Rebuilding a "clean" system while the compromised system is still functioning in order to maintain business continuity
- Preserving and handling evidence according to established procedures to maximize successful prosecution of the attacker(s)
- Keeping detailed documentation of all evidence including information about personnel who handle evidence or information, time and date of handling, locations where evidence stored, and security procedures for each step of evidence maintenance

Some organizations suggest NOT using normal shutdown procedures during an attack, as some operating systems—notably Windows—make many "writes" to the registry during the shutdown. Another potential issue regarding containment is that some attacks may cause additional damage when they are contained. For example, a compromised host may run a malicious process that pings another host periodically. When the incident handler attempts to contain the incident by disconnecting the compromised host from the network, the subsequent pings will fail. Because of the failure, the malicious process may overwrite all the data on the host's hard drive. Handlers should not assume that just because a host has been disconnected from the network, further damage has been prevented.

The NIST "Computer Security Incident Handling Guide" recommends coordinating with the legal department to determine if pursuing attackers legally is feasible and recommended. Gather evidence according to approved procedures and laws. Additionally, the SIRC and Forensics Technicians involved with an incident handling case should review NIST SP 800-86, **Guide to Integrating Forensic Techniques into Incident Response**, which provides detailed information on establishing a forensic capability. While that document focuses on forensic techniques for PCs, much of the material can apply to other systems.
If possible, try to identify attacking hosts. However, containment and the need to return to normal business operations is often more important. The SIRC and CISO should work with Executive Management to determine how best to prioritize these competing needs.

Containment steps:

- Deploy the containment team with specific instructions on how to approach the containment effort and emphasize their need to document their activities
- Secure all of the affected systems and areas
- Take sufficient time to investigate all services, workstations, networking equipment and other resources to ensure compromises are addressed in order to prevent a secondary outbreak
- Confirm and annotate that affected resources have synchronized clocks and, if not, note the time differences
- Determine need to order new equipment to replace compromised systems
- Backup and image systems before altering any of them
- Consider setting traps or honey pots if intending to identify and prosecute the attackers
- Do not log in to affected systems as an administrator or root
- Change all passwords on affected systems and services
- Acquire and review all available logs related to the attack, including logs from routers, servers, firewalls, applications, etc.
- Conduct a risk assessment on the attack and how to respond to it
- Document all activity
- Coordinate with legal counsel on the response team to determine:
  - Which state and federal laws and regulations are applicable ○ The probability that the information has been or will be misused ○ Contractual obligations of the organization to disclose the data breach ○ Whether regulators and customers need to be informed about the data breach, and developing the content of those communications

4.3 *PHASE 3: ERADICATION PHASE*

The primary goal during the eradication phase of incident response is to remove any evidence of the security incident from all network resources. Once an incident has been isolated and contained, teams should pursue an eradication strategy to remove all traces if it is an incident of an attack. It is imperative that the agency vigorously examines and eradicates all traces of the attack in case an attacker left behind Trojan horses or logic bombs to re-activate an attack after being reconnected to the network or Internet.

While it is difficult to list all steps to eradicate evidence, examples include:

- Deleting infected files
- Removing malware, such as Trojans and root kits
- Disabling compromised accounts
- Deleting bogus accounts
- Re-imaging infected systems
- Blocking vulnerable application ports
- Restoring compromised/corrupted operating system files
- Replacing physical data drives
- Performing a complete system re-install
- Improving physical security of equipment
- Installing surveillance equipment
- Changing host names, DNS entries, or IP addresses

It may also be practical during the eradication phase to install security controls to prevent similar future attacks. The response teams should implement appropriate protection techniques such as firewalls and/or router filters, moving the system to a new name/IP address, or in extreme cases, porting the machine's function to a more secure operating system.

Take steps to remove the cause of the exposure, reduce the impact of the exposure of the sensitive data, and ensure that future risk of exposure is mitigated.

4.4 *PHASE 4: RECOVERY PHASE*

Once the agency and COT response teams are sure that they have contained the incident, they must begin the recovery phase of the incident. This phase ensures that the system returns to operational status. It is possible, even likely, that some of these steps may be addressed during the eradication phase. Recovery phase steps may include:

- Restore the systems.
- Validate the systems. Once a system has been restored, verify that the operation was successful and the system is back to its normal condition.
- Decide when to restore operations. Management may decide to leave the system offline while operating system upgrades and patches are installed.
- Monitor the systems. Once the systems are back on line, continue to monitor for back doors that escaped detection.
- Harden the systems.
- Tighten network perimeter security.
- Ensure anti-virus software is installed and up-to-date

The type and scope of the security incident will dictate the recovery steps. Response teams need to determine whether to restore a compromised system or to rebuild the system or systems entirely. This will rely on presumably credible backups. Teams must make every effort to ensure uncorrupted data is restored to systems.

An incident could potentially corrupt data for many months prior to discovery. It is, therefore, very important that as part of your incident response process, you determine the duration of the incident.

4.5 *PHASE 5: POST-INCIDENT ACTIVITIES AND LESSONS LEARNED*

Once an agency and/or COT concludes handling a security incident, key participants should hold a wrap-up meeting to evaluate the incident and the incident handling policy and procedures. The SIRC should lead this wrap-up meeting (or series of meetings depending on the scale of the incident) and should develop a wrap-up incident report that includes detailed information about the incident, the response, and lessons learned. The agency and COT should use the report and lessons learned to:

- Identify key strengths and weaknesses of the response plan
- Identify gaps and fixes in security controls
- Identify practices for improvement
- Identify systemic security weaknesses
- Identify incident response policy and plan deficiencies
- Training new security team members
- Incorporate into new training and testing
- Update the incident response policy and procedures
- Improving end-user awareness by showing how their activities can affect the organizations security posture (e.g., a phishing scam that leads to widespread disruption)
- Notify appropriate personnel of need to improve their operations/applications/resources (e.g., default administrator password on a multi-function device, database, or network firewall)
- Maintain high-level documentation for prosecution or administrative discipline uses

Note: not all information from the wrap-up meeting and lessons learned can or should be shared with all users. Proper security of the incident's documentation is crucial.

Lessons learned documentation should include findings, recommendations, and proactive actions for COT and agencies to pursue. NIST Special Publication 800-53 (Revision 4), Security and Privacy Controls for Federal Information Systems and Organizations, recommends using the wrap-up meeting to determine the following and include in the lessons learned report:

- Exactly what happened, and at what times? What was the exact chronology of the incident and the response?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

This incident response plan should be reviewed and revised annually, incorporating changes from incident responses and the lessons learned during incidents.

APPENDIX – INCIDENT CLASSIFICATIONS

This section will describe many of the incidents to which an agency can expect to react, how to determine incident severity, incident declaration procedures, and an overview of how to handle the incidents. While this document cannot list all possible types of incidents, breaches, attacks, etc., it intends to provide guidelines for addressing them.

Virus/Worms

Viruses and worms in the Commonwealth's systems can be costly, especially in person-hours used to identify, isolate, and remediate the systems infected. Because worms are self-replicating and can spread widely and quickly, it is imperative to recognize and react to these attacks as quickly as possible. While viruses may not spread as easily and quickly, they can create significant damage and responders should address them as quickly as possible.

Virus and worm responses should include:

- Notify the appropriate personnel immediately.
- Notify front-line tech support personnel immediately, and then determine whether to declare the infection an incident for reporting to COT CISO and subsequent activation of response teams.
- Make a decision on isolating the infected devices. While disconnecting devices from the network will reduce/stop the spread of worms, it can also prevent access from remediation procedures, application patches, etc.
- Do not power off the infected device except as a last resort. Restarting systems infected with certain viruses can destroy data. Additionally, power cycling the system can lose information used in the forensics phase of researching the attack.

For forensics and remediation purposes, attempt to identify and isolate the suspected virus or worm-related files and processes. Save a snapshot of the systems' files and processes. If specific files that contain virus or worm code can be identified, move those files to a safe place—properly and conspicuously labeling the infected data to prevent re-introduction into the system or network—and then remove the infected files. Get a listing of all active network connections.

After isolating affected systems and documenting necessary virus/worm information, remediate the system. When possible, rebuild or re-image the system. However, if this is not a reasonable course of action due to system functions or criticality, confirm the removal of all suspicious files, services, processes, and registry entries. Update all operating system and application patches on the system. When returning the system to operational status, notify all affected or potentially affected personnel and agencies to alert them that a previously compromised system will be back online. As with all security incidents, responders must log all actions taken and prepare a follow-up report, which we will address later in this document.

Hacking Attempts

Some hacker-related incidents can include port scans, repeated login attempts, telnet or SSH attempts, unauthorized access, etc. Since hacker activity can cover a wide range of attacks, agencies and COT will need to address each one on a case-by-case basis. Regardless of the type of hacking attempts, we must respond to them appropriately, as a successful attack can lead to more severe security breaches. Some basic response procedures for hacking attempts include:

- Begin a log detailing all actions related to the hacking attempts. Include information from reviewing system logs, all active network connections, and copying all audit trail information. In addition, record any other files, processes, or logs that can help identify and remediate any issues or that can aid in subsequent criminal prosecution.
- If an agency encounters an active session by a hacker/unauthorized person, authorities must

decide whether to allow the session to continue for forensic and criminal prosecution reasons. However, time is critical due to the potential for damage or data breaches. Since maintenance of forensic data is critical, we recommend disconnecting the compromised system from the network rather than powered off.

- As with other incidents, any vulnerability that led to the attack must be addressed. Ensure only legitimate user accounts are on the system and that passwords are changed. If possible, rebuild the system from a clean image.

Phishing and e-mail fraud

Phishing and e-mail fraud are becoming very prevalent in the Commonwealth's systems. These attempts to acquire personal or sensitive data or financial information from seemingly legitimate companies or users can create significant issues, especially if an unsuspecting user provides usernames or passwords for Commonwealth systems. Increasingly sophisticated technical abilities by criminals and black hats, coupled with some users' lack of awareness and vigilance, create potential detrimental conditions for agencies.

Countermeasures for phishing and e-mail fraud must include an ongoing awareness/education program by COT and agencies. Policies and procedures can address this to a degree, but each agency should also include periodic alerts, e-mails, seminars, etc. as part of the ongoing awareness program.
If COT, an agency, or a user should realize that a user clicked on a suspected phishing scam link, some basic response procedures apply.

Notify COT, via the Commonwealth Service Desk, of the phishing attempt. COT Security Office requires a copy of the e-mail, not a forwarded e-mail, for research and mitigation purposes. To do this in Outlook, for example:

- Highlight the suspicious e-mail
- In the Outlook menu bar, select "Edit/Copy"
- Open a new email and "Paste" the suspicious e-mail into the body
- Provide a descriptive subject in e-mail (e.g., "Suspected Phishing Attempt)
- In the body of the notification e-mail, give a brief description of the issue (e.g., "I received the attached e-mail from an unknown agency that looks suspicious. Please forward to the Security Office for review."
- Send to **CommonwealthServiceDesk@ky.gov**
- Delete original suspicious e-mail from Inbox and Deleted Items folders

COT/agencies must change the passwords on any accounts that the phishing attempt compromised or potentially compromised. Agency personnel must scan and remediate any security issues on the machine on which a user responded to a phishing attempt. COT E-mail team must disconnect the mailbox of any user account that responds to any phishing attack until the user's workstation has been cleared of any infection.

Data Breaches

There can be several types of data breaches in the Commonwealth's network, and each type of data breach may require different approaches to addressing through the Incident Handling procedures. There can be breaches of non-sensitive data, PII data, state-owned data, federal data, and health care data (e.g., HIPAA: Health Insurance Portability and Accountability Act). Regardless of the type of breach, agencies and COT must work together to contain and mitigate the breach while addressing the unique data accessed. As a rule, when agencies suspect potential or actual data breaches, they should not access the system until a technician creates a forensics copy of the system.

Wireless Incidents

Most incidents that attack the wireless networks can be addressed the same as attacks over wired connections, such as viruses, phishing scams, etc. However, it is possible that an attacker can manipulate the agency's wireless network by installing rogue devices or accessing the agency's network through improperly placed or

misconfigured devices. Agencies must be vigilant in monitoring for rogue devices and must review and configure wireless devices to ensure only authorized users can access Commonwealth networks and resources. If a rogue device is found on a Commonwealth network, the agency should contact the Commonwealth Service Desk immediately.

Social engineering

Social engineering attacks can be a precursor to almost every other kind of attack. Through social engineering, attackers can acquire legitimate credentials and consequently conduct man-in-the-middle attacks, data breaches, network and resource disruption, etc. It is imperative that agencies advise employees about social engineering techniques and provide regular awareness training. Employees must be conscious of shredding documents with sensitive data, ensuring others do not "tailgate" into secure facilities, not clicking on suspicious links or visiting suspicious websites, confirming the identities and purposes of callers, and other potential attempts at social engineering.

Physical property attacks

There can be a wide variety of physical property attacks, so response procedures for each one will be handled by the agency. These attacks, such as mobile device theft, destruction of agency resources, and others, may require involvement by other agencies, law enforcement, or other entities. The incident response team will determine how to handle each of these incidents. However, general response procedures may include remote wipe of stolen devices, video monitoring review, and other forensic techniques to identify attackers and mitigate data/resource loss. Moreover, when keys or badges are lost or stolen, employees and/or agencies much contact COT immediately to take appropriate precautions and countermeasures.

APPENDIX – SAMPLE PRESS RELEASE

State officials announced that a security breach of the state's network resources has been detected. Immediate steps have been taken to stop the breach and an investigation is currently underway. As this is an ongoing investigation, limited information can be shared.

However, agencies currently affected by the breach include the _____ Cabinet, the _____ Cabinet, and the Department of _____. Those who are potentially affected have been (or are in the process of being) notified. More details will be released as the in-depth investigation continues.

The (database, server, workstation) contained some personal information of state (employees, Commonwealth citizens), although no (health care data, social security numbers) are known to have been compromised. State security personnel discovered that the attack occurred between (date/time) and (date/time) at the (Office of _____).

State officials believe that this breach creates a (low, medium, high) risk to the state's (employees, constituents), but wanted to alert those who may potentially be affected. Security and network personnel have isolated the breach, and will continue to investigate this attack and work with law enforcement.

Affected individuals may call (1-800-XXX-XXX) for more information. In addition, the state will provide updates of the security breach and response at the www.ky.gov website.

APPENDIX – INTERNAL SAMPLE SECURITY ALERT

ALERT!

A Severe Security Incident Has Occurred

To all personnel,
COT employees identified a security breach/attack beginning on ____ (date) ____ and are currently responding to and investigating the breach. COT notified the appropriate agencies and authorities and will notify media to help disseminate information when necessary.

Please be aware of the incident and stay alert for indications of the attack. We ask that you notify your management if you identify any suspicious activity.

To insure that timely and accurate information is made available to the media and public, COT management will coordinate the state response. Should you be notified by media, please inform your supervisor. Giving out unauthorized information could jeopardize work on fixing the breach as well as the ongoing investigation.

Please do **NOT** send any information about the breach electronically unless specifically asked to do so or unless secure communications are available.

For more information, please contact your management.

ALERT!

APPENDIX – DATA BREACH OVERVIEW AND LINKS

Social Security Administration (SSA)
States and other entities that have entered into an electronic information sharing agreement with the Social Security Administration (SSA), collectively referred to as Electronic Information Exchange Partners (EIEP). The Commonwealth Office of Technology (COT) is considered an Electronic Information Exchange Partners (EIEP) from an information technology standpoint as it hosts electronic information.

If EIEP experiences or suspects a breach or loss of PII or a security incident that includes SSA-provided data, they must notify the United States Computer Emergency Readiness Team (US-CERT) within one hour of discovering the incident. The EIEP must also notify the SSA Systems Security contact named in the agreement. If within 1 hour the EIEP has been unable to make contact with that person, the EIEP must call SSA's National Network Service Center (NNSC) toll free at 877-697-4889 (select "Security and PII Reporting" from the options list). The EIEP will provide updates as they become available to SSA contact, as appropriate. Refer to the worksheet provided in the agreement to facilitate gathering and organizing information about an incident.

IRS Publication 1075 http://www.irs.gov/pub/irs-pdf/p1075.pdf

The IRS Publication 1075 (Pub 1075) provides guidance to ensure the policies, practices, controls, and safeguards employed by recipient agencies, agents, or contractors adequately protect the confidentiality of Federal Tax Information (FTI). Enterprise security policies address the purpose, scope, roles, responsibilities,

management commitment, coordination among organizational entities, and compliance to implement all applicable security controls. Pub 1075 contains the managerial, operational, and technical security controls that must be implemented as a condition of receipt of FTI.

A mutual interest exists in the responsibility to ensure that FTI is disclosed only to persons authorized and used only as authorized by statute or regulation. It is the agency's responsibility to ensure all functions within the agency, including consolidated data centers and contractors (where allowed by federal statute) with access to FTI, understand and implement the requirements in this publication.

This publication provides the preliminary steps to consider before submitting a request to receive FTI, requirements for proper protection, expectations from the IRS, and considerations that may be helpful in establishing a program to protect FTI. The exhibits in this publication are provided for additional guidance.

Criminal Justice Information Services (CJIS) Security Policy
http://www.kentuckystatepolice.org/cjis/pdf/security_policy_rev_07_12.pdf

The CJIS Security Policy provides Criminal Justice Agencies (CJA) and Noncriminal Justice Agencies (NCJA) with a minimum set of security requirements for access to Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Division systems and information and to protect and safeguard Criminal Justice Information (CJI). Its minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJIS Security Policy is to provide the appropriate controls to protect CJI, from creation through dissemination, whether at rest or in transit.

The CJIS Security Policy integrates presidential directives, federal laws, FBI directives, the criminal justice community's Advisory Policy Board (APB) decisions along with nationally recognized guidance from the National Institute of Standards and Technology (NIST) and the National Crime Prevention and Privacy Compact Council (Compact Council).

Information Security Officers are identified as the points of contact on security-related issues for their respective agencies and shall ensure Local Agency Security Officers institute the CJIS System Agency incident response reporting procedures at the local level.

The agency shall promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the agency shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the designated point of contact.

KRS 61.931 – 61.934– Personal Information Security and Breach Investigations
Kentucky passed a new bill in 2014 that enforces data-security requirements, investigation requirements and breach notification requirements on governmental agencies and "nonaffiliated third parties" that do business with governmental agencies. The law is effective January 1, 2015.

The requirements have been created as a new section of KRS Chapter 61 to require public agencies and nonaffiliated third parties to implement, maintain, and update security procedures and practices, including taking any appropriate corrective action to safeguard against security breaches. The bill will also require entities to establish reasonable security and breach investigation procedures, which include contracts with nonaffiliated third parties. Public agencies that maintain personal information are required by law to notify those impacted by security breaches. They will need to notify specified officials of security breaches and specify

how to provide notice of security breaches to impacted individuals. The Department for Libraries and Archives must establish procedures for the disposal and destruction of records that include personal information. The Commonwealth Office of Technology has a security framework in place, but will now be required to submit an annual report to the Legislative Research Commission regarding security breaches.

.931 Definitions for KRS 61.931 to 61.934. (Effective January 1, 2015)

.932 Personal information security and breach investigation procedures and practices for certain public agencies and nonaffiliated third parties. (Effective January 1, 2015)

.933 Notification of personal information security breach -- Investigation -- Notice to affected individuals of result of investigation -- Personal information not subject to requirements -- Injunctive relief by Attorney General. (Effective January 1, 2015)

.934 Personal information security and breach investigation procedures and practices for legislative and judicial branches -- Personal information disposal or destruction procedures. (Effective January 1, 2015)

APPENDIX – DATA BREACH TEMPLATES

Notification Template

Date

TO: Agency Name
Agency Address
Agency Address
Agency Address

RE: Potential Information Exposure

TO WHOM IT MAY CONCERN:

The Commonwealth of Kentucky and (the Agency Cabinet) is hereby notifying you of the potential exposure of confidential Cabinet information. The Cabinet recently discovered that [include information about the security breach, for example, a description of the categories of information that were subject to the security breach, including the elements of personal information that were or were believed to be acquired]. The security hole has since been plugged, and the data documentation is no longer vulnerable.

Given the structure of the system, any unauthorized access would have required technical expertise. The Cabinet [include whether reason exists, or not - has no reason] to believe that the documents and/or data were actually viewed by anyone without appropriate credentials. However, that possibility cannot be definitively ruled out; thus we are taking the precaution of notifying you and affected individuals. All individuals whose

personal information as defined in KRS 61 was potentially exposed, will be informed of the incident and provided with information about how to monitor their credit to help protect against identify theft.

We will begin notifying affected individuals on _____. Please let us know by close of business on _____ if you request that such notice be delayed to facilitate investigative efforts.

Sincerely,

Notification Template

Date

TO: Agency Name
Agency Address
Agency Address
Agency Address

RE: Potential Information Exposure

To Whom It May Concern:

The Commonwealth of Kentucky and (the Agency Cabinet) is hereby notifying you of the potential exposure of confidential Cabinet information. The Cabinet recently discovered that [include information about the security breach, for example, a description of the categories of information that were subject to the security breach, including the elements of personal information that were or were believed to be acquired]. The security hole has since been plugged, and the documentation and/or data is no longer vulnerable.

Given the structure of the system, any unauthorized access would have required technical expertise. The Cabinet [include whether reason exists, or not - has no reason] to believe that the documents or data were actually viewed by anyone without appropriate credentials. However, that possibility cannot be definitively ruled out; thus we are taking the precaution of notifying you and affected individuals. All individuals, whose personal information as defined in KRS 61 was potentially exposed, will be informed of the incident and provided with information on how to monitor their credit to help protect against identify theft.

We will begin notifying affected individuals on _____.

Sincerely,

Citizen Template for Social Security Number (SSN) Exposure

Date

Dear:

We are writing to you because of a recent computer security incident at the Commonwealth of Kentucky. [Describe what happened in general terms, what kind of PII was involved, and what you are doing in response.]

To protect yourself from the possibility of identity theft, we recommend that you complete a Federal Trade Commission (FTC) ID Threat, located on their web site at http://www.consumer.ftc.gov/features/feature0014-identity-theft. This will allow you to notify your creditors legally that your identity may have been compromised.

You are encouraged to contact the Office of the Attorney General, 700 Capitol Avenue, Suite 118, Frankfort, KY 40601-3449. Their web site is located at http://ag.ky.gov/Pages/default.aspx, and their phone number is 502.696-5389.

We also recommend that you place a fraud alert on your credit files. A fraud alert lets creditors know to contact you before opening new accounts. Just call any one of the three credit reporting agencies at the number below. This will let you automatically place fraud alerts. You should receive letters from them, with instructions on how to get a free copy of your credit report.

Equifax	Experian	TransUnion
1-888-548-7878	1-877-284-7942	1-800-916-8800

Please review your credit reports carefully when you receive them. Look for accounts you did not open, for inquiries from creditors that you did not initiate, and for personally identifiable information, such as home address or Social Security Number, that is not accurate.

If there is anything you do not understand, call the credit-reporting agency at the telephone number on your report. If you do find suspicious activity on your credit reports, you need to call your local police or sheriff's office to file a police report of identity theft. [Alternatively, if appropriate, give contact information for law enforcement agency investigating the incident.] We suggest you get a copy of the police report, as it may be helpful in clearing up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you continue to check your credit report every three months for the next year. Call one of the numbers above to order your reports and keep the fraud alert in place. For more information on identity theft, we suggest that you call FTC toll free at (877) 382-4357 and/or visit their Identity Theft Web Site at http://www.consumer.gov/idtheft/.

Should you have further questions or need additional information,, please call us anytime at our toll free number, _____.

Sincerely,

Template for Data Breach Call Center Procedures

In the event of a significant data breach involving Personally Identifiable Information (PII), the following guidance is provided in regard to establishing a call center. The purpose of a call center is to provide a number for individuals to call to obtain further information regarding the data loss and possible action to take to lessen the incident's impact on their personal lives.

The decision to establish a call center should be based on several considerations:

- Each situation will be unique, and the decision to establish a call center must be based on individual circumstances. The main concern should be sharing of information with those affected and how they may obtain assistance.

- If a data breach does not extend outside of the agency (i.e., those affected by the breach can easily be contacted), the establishment of a call center may not be necessary.

- If the breach affects a large number of individuals and those individuals are not easily contacted, establishing a call center should be considered to allow potentially impacted customers to call for additional information regarding the breach.

Once a decision is made to establish a call center, there are several options:

- While KRS 61.931-934 does not require a toll-free number, it would be helpful for widespread required notices.

- To establish a fully supported and staffed call center, be sure to include a thorough description of the incident and a set of Frequently Asked Questions (FAQs) for the call center to refer to when fielding calls (suggested FAQs are provided in this document).

- Some items to consider based on the nature of the breach include:

- Using existing personnel to staff the call center
- Training of call center operators
- Ability to adjust staffing in response to call volume
- Daily hours of operations
- Call logging
- Reporting requirements
- Advertising call center number(s) and making data breach information readily available to those affected
- Quality assurance checks of call center effectiveness

Sample ***Data Breach Call Center Frequently Asked Questions (FAQs)***

Q: How can I tell if my information was compromised?

At this point, there is no evidence that any missing data has been used illegally. However, the _____ is asking each individual to be extra vigilant and to carefully monitor credit card statements, bank statements, and any statements relating to recent financial transactions. If unusual or suspicious financial activity is noticed, you should report it immediately to the financial institution involved.

Q: I haven't noticed any suspicious activity in my financial statements, but what can I do to keep myself from being victimized by credit card fraud or identity theft?

The _____ strongly recommends that individuals closely monitor their financial statements and visit the _____ special web site at _____.

Q: What is the earliest date when suspicious activity might have occurred due to the breach?

The information was stolen from an employee of the _____ during the month of _____. If the data has been misused or otherwise used to commit fraud or identity theft crimes, it is likely that individuals may notice suspicious activity during the month of _____.

Q: Should I reach out to my financial institutions or will the _____ do this for me?

The _____ does not believe that it is necessary to contact financial institutions or cancel credit cards and bank accounts, unless you suspicious activity is detected.

Q: Where should I report suspicious or unusual activity?

The Federal Trade Commission (FTC) Identify Theft web site at http://www.consumer.ftc.gov/features/feature-0014-identity-theft recommends the following steps if you detect suspicious activity:

a. Immediately place an Initial Fraud Alert by contacting the fraud department of one of the three major credit bureaus:

   Equifax: 1-800-525-6285; www.equifax.com; POB 740241, Atlanta, GA 30374-0241

   Experian: 1-888-EXPERIAN (397-3742); www.experian.com; POB 9532, Allen, TX 75013

   TransUnion: 1-800-680-7289; www.transunion.com; POB 6790, Fullerton CA 92834-6790

b. Order Your Credit Report from the three major credit bureaus above.

c. Create an Identity Theft Report. Submit a report about the theft to the FTC online or call the FTC at 1877-438-4338 (1-866-653-4261 – TTY). When you finish writing all the details, print a copy of the report. It will be called an Identity Theft Affidavit. Take your FTC Identity Theft Affidavit with you when you file a police report with your local police department or the police department where the theft occurred.

d. Extended Fraud Alerts' Information: If you've created an Identity Theft Report, you can get an extended fraud alert on your credit file. When you place an extended alert, you can get two free credit reports within 12 months from each of the three credit reporting companies. The credit reporting companies must take your name off marketing lists for prescreened credit offers for five years, unless you ask them to put your name back on the list. The extended alert lasts for seven years.

e. Credit Freezes' Information: You may choose to put a credit freeze on your file. But a credit freeze may not stop misuse of your existing accounts or some other types of identity theft. Also, please note that companies that you do business with would still have access to your credit report for some purposes. A fraud alert will allow some creditors to get your report as long as they verify your identity.

   Note: Close any accounts that have been tampered with or opened fraudulently.

Q: What is the _____ and/or others doing to ensure that this does not happen again?

The _____ is working with the FTC to investigate the data breach and to develop additional safeguards against similar incidents. Employees have been directed to complete a Security Awareness course. Also, appropriate law enforcement agencies, including the Office of Attorney General, have launched full-scale investigations into this matter.

Q: Where can I get further, up-to-date information?

We have set up a special web site which includes up-to-date news and information. Please visit _____ _____.

Q: Does the data breach affect only certain individuals?

It potentially affects a large population of individuals. We urge everyone possibly affected to be extra vigilant and monitor their accounts.

REFERENCES

Enterprise Polices and link to Incident Response Policy:

http://technology.ky.gov/governance/Pages/policies.aspx

NIST Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf

NIST Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide"

http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

NIST Special Publication 800-86, "Guide to Integrating Forensic Techniques into Incident Response"

http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf

KRS 42.724, Creation and authority of Office of the Chief Information Security Officer

KRS 42.726, Roles, duties, and permissible activities for Commonwealth Office of Technology -- Duties of Archives and Records Commission and Department for Libraries and Archives not affected -- Annual report concerning security breaches KRS 61.931, Definitions for KRS 61.931 to 61.934

KRS 61.932, Personal information security and breach investigation procedures and practices for certain public agencies and non-affiliated third parties

KRS 61.933, Notification of personal information security breach -- Investigation -- Notice to affected individuals of result of investigation – Personal information not subject to requirements -- Injunctive relief by Attorney General

200 KAR 1:015 Data Breach Notification Forms

Finance Form Site for Data Breach Notification:

http://finance.ky.gov/SERVICES/FORMS/Pages/default.aspx NIST Special

Publication 800-61, Computer Security Incident Handling Guide

http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf