Incident Response Plan for PCI-DSS Compliance

Office of the UK Chief Security Officer
October 25th, 2009

I. Policy

The UK IT Security Office (ITSO) is responsible for responding to reports of incidents, compromises and breaches of UK computers, data, and network resources. The purpose of the Incident Response Plan is to establish procedures in accordance with applicable legal and regulatory requirements to address instances of unauthorized access to or disclosure of University information. The Incident Response Plan defines the policy, roles and responsibilities for the involved personnel when reacting to an information security threat.

The primary emphasis of activities described within this plan is the return to a secure state as quickly as possible, while minimizing the adverse impact to UK. Depending on the circumstances, the ITSO may decide to modify or bypass one or more of the procedures outlined in this plan in response to a particular security incident, with the understanding that the ITSO will take all reasonable steps to investigate and resolve any security issues. The capture and preservation of incident relevant data (e.g., network flows, data on drives, access logs, etc.) is performed primarily for the purpose of problem determination and resolution, as well as classification of the incident.

The University shall provide timely and appropriate notice to affected individuals and departments when there has been a security incident, a compromise or a breach involving UK data, computers or networks. The Chief Security Officer and the Office of Legal Counsel, shall be responsible for reviewing breaches to determine whether notification is required, and directing responsible departments in complying with the notification obligation. All known or suspected security incidents must be reported to the CSO. Suspected incidents can be reported at security@uky.edu or the IT CSC help-desk.

II. Definitions

Security Incident - A vulnerability which may compromise the security of university resources has been discovered and is underway. Generally, this means a weakness in intrusion prevention has been found, an attempted exploit has taken place, or reconnaissance by a hacker has been thwarted. Examples include systematic unsuccessful attempts to gain entry, a PC or workstation infected with a virus, worm, Trojan, botnet, or other malware that has been discovered and removed.
Security Compromise – An escalation of a security incident where the attacker has gained control of a university account, system or device, and is leveraging that position to control and utilize compromised resources for the purpose of unauthorized acquisitions. At this point, it has been determined that data has not been compromised or stolen.

Security Breach – A confirmed, unauthorized acquisition, modification or destruction of University or private data has taken place. At this point, a breach has been forensically determined and evidence supports that data was compromised.

Private data – Data about individuals that is classified by law as private or confidential and is maintained by the University in electronic format or medium. “Private data” means data classified as not public and available to the subject of the data, and "confidential data" means data classified as not public but not available to the subject of the data.

Unauthorized acquisition – For the purposes of this plan, this means that a person has obtained University data without statutory authority or the consent of the individual who is the subject of the data, and with the intent to use the data for non-University purposes.

Systematic unsuccessful attempts – Continual probes, scans, or login attempts, where the perpetrators obvious intent is to discover a vulnerability and inappropriately access and compromise that device.

UK IT Resources or Systems – includes all University-owned computers, peripherals, networks and related equipment and software, and the voice and data communications infrastructure.

The UK Information Technology Security Office (ITSO) – a unit within the UK Information Technology department. The mission of the ITSO is to provide proactive security analysis, development, guidance and education.

The ITS Incident Response Team – members of the ITSO, who receive, triage, resolve, classify and track incidents of technology abuse or security issues for the entire UK enterprise. The ITSO coordinates the efforts of the SECSWAT team, as well as external Internet Service Providers, law enforcement agencies and other institutions.

III. General Incident Response Procedures

1) Intrusion attempts, security breaches, or other technical security incidents perpetrated against UK-owned computing or networked resources must be reported to the IT Security Office. Functional unit managers and/or systems personnel must:

   a) Report any security incidents in order to obtain assistance and advice, or to file the incident in the SECSWAT database.
   b) Report any systematic unsuccessful attempts (e.g., login attempts, probes or scans).
   c) Where feasible given the circumstances, reports should be sent as soon as the situation is detected; minimally the report should be sent as soon as possible thereafter.
2) Upon receiving a report of a security incident, the IT Security Office will:
   a) Ensure that appropriate information is collected and logged per applicable procedures.
   b) Immediately assess actual or potential disclosure or inappropriate access to institutional or personal information.
   c) Report the situation to the University IT Chief Security Officer.
   d) Consult with and/or assign the incident to an ITSO security engineer for further investigation as necessary.
   e) Provide preliminary advice or comment to the functional unit technician as required.
   f) Initiate steps to warn other University of Kentucky systems personnel if it appears that the situation has the potential to affect other University systems as well.
   g) Perform or assist in any subsequent investigation and/or perform computer forensics as required.

3) Upon receiving a report of a security incident, the UK IT Chief Security Officer will:
   a) If circumstances dictate, report to the Chief Information Officer (CIO) and Chief Technology Officer (CTO).
   b) If circumstances dictate, contact the senior manager of the department or agency involved.
   c) If circumstances dictate, report and/or consult with UK Legal Counsel, UK Police, Internal Audit, UK Public Relations or other appropriate agencies.
   d) Ensure that appropriate records are filed.
   e) Confirm actual or probable disclosure or inappropriate access to institutional or personal information.
   f) Invoke formal incident response procedures commensurate with the situation.

4) The Functional Unit managing a system that has had an incident, has been compromised or breached is ultimately responsible for making the determination if the system will be only restored and operations resumed, or if pursuit of the perpetrator is feasible and appropriate based on possible continued affect on operations. Such investigation may be requested by law enforcement, and UK Legal Counsel must be consulted to see if any such request is legally binding before a contrary decision is made to only recover the system and restore the service.

5) The Functional Unit managing a system that has had an incident, has been compromised or breached is responsible for all monetary, staff, and other costs related to investigations, cleanup, and recovery activities resulting from the compromise, response, or recovery.

6) In order to protect UK data and systems, as well as to protect threatened systems external to the University, the UK Security Officer may block, or place restrictions on technology services provided using any University owned systems and networks. Specifically:
   a) Limitations may be implemented through the use of policies, standards, and/or technical methods, and could include (but may not be limited to) usage eligibility rules, password requirements, or restricting or blocking certain protocols or use of certain applications known to cause security problems.
   b) Restrictions may be permanently deployed based on a continuing threat or risk after appropriate consultation with affected constituents, or they may be temporarily deployed, without prior coordination, in response to an immediate and serious threat.
c) Restrictions deployed temporarily will be removed when the risk is mitigated to an acceptable level, or where the affect on University functions caused by the restriction approaches or exceeds risk associated with the threat, as negotiated between the affected constituents and the IT Security Officer.

7) In order to protect University data and systems, as well as to protect threatened systems external to the University, the UK IT Security Officer may unilaterally choose to isolate a specific University system from campus or external networks, given:

a) Information in-hand reasonably points to the system as having been compromised.

b) There is ongoing activity associated with the system that is causing or will cause damage to other University systems and/or data, or the assets of other internal or external agencies, or where there is a medium-to-high risk of such damage occurring.

c) All reasonable attempts have been made to contact the responsible systems personnel or department management, or such contact has been made where the technician or department managers are unable to (or choose not to) resolve the problem in a reasonable time.

d) Isolation is removed when the risk is mitigated to an acceptable level, or where loss of access or function caused by the isolation approaches or exceeds risk associated with the threat, as negotiated between the responsible functional manager and the IT Security Officer.

e) Advance consultation with the appropriate campus Chief Information Officer or Legal Counsel, where practical and where circumstances warrant.

8) The reaction to a reported security vulnerability directly corresponds to the potential for damage to the local system (or adjacent systems) or inappropriate disclosure or modification of data. The risk levels are characterized as:

a) Very High Risk, response is immediate:

1. Damage to the system or data is occurring, or
2. Attempts to exploit the vulnerability on that system are occurring, or
3. The vulnerability is currently being actively exploited against other similar technologies within the University; probable damage to systems and data is being experienced in those other incidents.

b) High Risk, response is within 1 hour:

1. The vulnerability is known to exist on the system;
2. The exposure is currently being actively exploited against other similar technologies external to the University;
3. Damage to systems and data are being experienced in those other incidents.

c) Medium Risk, response should be within 4 hours:

1. The system is susceptible to the vulnerability given that the system is configured incorrectly;
2. The exposure is currently being actively exploited against other similar technologies external to the University;
3. There is some potential for damage to systems and data.

d) Low Risk, response should be within 8 hours:

1. The system is susceptible to the vulnerability given that the system is configured incorrectly;
2. The exposure is currently being actively exploited against other similar technologies external to the University;
3. Damage to systems and data is possible but is not considered likely.

9) In the event of a significant series of incidents, a compromise or a breach, the entire episode and response are reviewed to determine which parts of the ITSO plan worked correctly. The “lessons learned” will be part of an After Action Review to determine areas that need to be changed (policies, system configurations, etc.).

10) Reports of security incidents should be sent to security@uky.edu The policies, security resources and other related materials can be found at: http://www.uky.edu/IT/Security.

IV. Procedures for System Administrators

1. **Don't panic.** Be as calm and methodical as you can, and think about your course of action. Involve a second person to assist and observe all actions you take.

2. **Do a quick assessment.** Do not immediately shut down the machine, as you may lose important information. If the machine is being used to attack others, or if the attacker is actively using or damaging the machine, you may need to disconnect it from the network. If this does not appear to be the case, leave the system intact for the moment.

3. **Report the problem.** Call the IT Security Office (859-257-2200) or the IT Customer Service Center (859-257-1300), and request an emergency system security check. This information will help you to assess the damage. (The machine must be up and on the network in order to run the tools.) Alternatively, you can send a message (using a different PC) to security@uky.edu or contact the CSC Help Desk at 7-1300. Every effort will be made to respect the confidentiality of incident information.

4. **Gather all the relevant information you can find.** This may include, but is not limited to, system logs, directory listings, electronic mail files, screen prints of error messages, and database activity logs. Copy them to a safe location (that will not be deleted or over-written), so that you can study them later.

5. **Take notes.** Have your partner record all relevant information, including things you observed, actions you took, dates and times, and the like. It is best to log your activities as they occur. Over time, your actions and the order in which they were executed will not be
easily remembered. The preservation of information is critical to any legal action that may take place at a later date.

6. **Change account passwords.** All system accounts that were involved with the incident should have new passwords. Exceptions to this rule are accounts which are authenticated with tokens or certificates, in which case the PIN or pass-phrase for them should be changed. **Never** share your password (pin, or pass-phrase) with anyone, for any reason. Choose a strong password and change it often.

7. **Change the status of accounts, if necessary.** In the event that a system administrator detects a problem with a system, or user activity on a system, a quick way to stop the unwanted activity is to "close" an account, by restricting logins to it. This results in the account owner having to contact an administrator in order to remove the login restriction. This is *not* deleting the account, but is merely making the account temporarily unusable.

8. **Stop rogue service(s), if necessary.** In the event that a system compromise or denial-of-service attack is underway, and you are unable to stop or kill the service(s), you may need to disconnect the machine from the network to get them stopped.

9. **Review your backup policies.** If you believe your data and/or operating system has been compromised, you must ensure that a "clean" backup is available for restoration. If your next backup *could* overwrite an undamaged backup, take *immediate* steps to prevent that occurrence. If your policy includes multiple levels of backup, and you are uncertain how long the system has been compromised, you must determine which backup to version restore to. Until that time, do not allow any backups to be overwritten.

10. **Decide on a course of action for repair.** The appropriateness of each course of action varies with the severity of the incident, (amount of damage, legal implications, cost of recovery, etc) and in the case of department-owned systems, the department policy. The IT Security Office staff will advise you in making a decision about the correct course of action. Advice about additional protections that can be applied to your system to prevent future problems is also available.

If you have questions about incident procedures, contact security@uky.edu