Incident Checklist

Sensitive Data Exposure Incident Checklist

Version 1.1: May 2013

We recommend reading the purpose statement, introduction, overview, and suggestions for how to use the checklist before downloading a copy.

Purpose

To provide a toolkit that includes resources, procedures, and guidelines for the management of incidents involving the exposure of sensitive and/or personal information. Complementary to the Data Incident Notification Toolkit, this information can be referred to during the process of responding to incidents that create the need for such notification.

Introduction

The following information is intended to provide a general checklist of the steps that an institution might take when an incident involving sensitive data is discovered. Although each item is recommended as an effective practice, we recognize that state/local legal requirements, institutional policy, or campus culture might cause each institution to approach this process differently. State legislation regarding incident breach varies broadly and institutions should check with legal counsel in advance to ensure this checklist meets statutory need. Institutions will also be at varying stages of progress in their incident response management capabilities. Some will start with the need to establish actions in the areas of policies, processes, or tools, some will be ready to implement, and others will be able to revise and fine-tune their processes. This checklist can be helpful for all, as a review of readiness or as a roadmap for development.

Checklist Overview

The checklist consists of the five major steps described below, with sub-steps included for each.

>>STEP 1: Identification

Verify that an incident has actually occurred. This activity typically involves the Unit systems administrator and end user, but may also result from proactive incident detection work of the Security Office or central IT operations. If it is determined that an incident has occurred, inform appropriate authorities.

>>STEP 2: Damage Containment and Data Exposure Assessment

Identify an Incident Response Lead and assemble an incident response team charged with limiting further damage from the incident. Conduct a thorough assessment of the type and scope of data exposed following applicable laws, regulation and policy.

>>STEP 3: Eradication and Recovery

Take steps to remove the cause of the exposure, reduce the impact of the exposure of the sensitive data, restore operations if the incident compromised or otherwise put out of service a system or network, and ensure that future risk of exposure is mitigated.

>>STEP 4: Notification

Determine the need to give notice to individuals whose data may have been exposed by the incident. Swiftness in notifying those affected by a breach of personally identifiable information (PII), as well as informing certain government entities, is legally mandated in many states and, depending on the nature of the data, also federal law. Speed is also important from a public relations standpoint. To this end, many of the sub-steps can and should be undertaken in parallel to accommodate these needs.

>>STEP 5: Follow-up

Identify lessons learned from the incident, implement any remediation needs, and securely store a complete record of the incident.

How To Use

Depending upon the nature of the incident and size of the response team, it may be advisable and practical to address some of the checklist steps and sub-steps in parallel. For example, as soon as the cause of an incident is determined (Step 2.6), eradication of that cause and recovery of the function it put out of service (Step 3) could commence while documentation activities of Step 2.7 are being addressed. The potential for multitasking incident steps and sub-steps is depicted in this workflow.

In ways similar to emergency preparedness planning, it is wise to periodically practice the institution's security incident response readiness in advance of actual events. Lessons learned should be incorporated as needed into the checklist, response procedures, and/or resource allocations.

The checklist includes actions needed to address the most serious of security incidents, i.e. the exposure of personally identifiable information (PII) protected by laws, industry standards, and/or contracts with parties external to the institution. It can also be used effectively to address other security incident types, e.g., defacement of public websites, unauthorized access to confidential but not legally protected data, or the loss of confidential paper records.

As helpful as we hope this checklist will be, it is important to consider that:

- Breach notification requirements are dictated by laws and industry standards that have and will continue to change over time. Contracts with third parties, such as, research fund granting organizations, may also bound institutions to additional notification requirements. This checklist includes

requirements for the most broadly applicable regulations, e.g. Payment Card Industry Data Security Standards, the Health Insurance Portability and Accountability Act, and the Family Educational Rights and Privacy Act. For the stated reasons, however, there may be other requirements institutions will need to incorporate.
- Given the trend toward increased use of external third parties, including cloud computing vendors, for providing services that use, collect, store, and/or process institutional data, institutions must take into account the shared responsibilities for incident response often necessitated by such arrangements. This checklist provides steps that must occur regardless of the location of a potential data breach. Who should assume responsibility for each of those step when a third party is involved will vary depending upon the nature of the external service provided, as well as the security-related terms of the contract between the institution and that party.

Training and Tools

In addition to establishing a coordinated, repeatable process for incident response (which this checklist facilitates), access to trained technical professionals and tools are also needed for effective incident response. While there is an abundance of security consulting firms available to supply these needs, institutions may find it more cost-effective to train and equip their own staffs to address incidents on an ongoing basis.

Training – There are many good sources of both management and technical training in computer incident handling techniques. The SANS Institute, for example, provides a number of courses (at this writing, six on the specialty of computer forensics alone). Training is also offered by some academic institutions and, of course, by many technical training vendors.

Tools – Likewise, there is a wide range of incident response tools from both commercial and open source origins. Categories include but are not limited to:

- *Scanning tools* – These identify incident artifacts and/or characteristics of vulnerabilities that help gauge the scope of a given incident. Examples are: OS fingerprinting, TCP/UDP port scanning, and software vulnerability scanning.
- *Acquisition tools* – These copy data in pristine condition for later analysis. The scope of acquisition sits on a broad range: from a single file, to random access memory, to entire hard drive, and so on.
- *Analysis tools* – These help determine the behavior of unwanted activity, e.g., malicious insider activity and malware, so that conclusions can be reached regarding impact and needed remediation actions. A few examples are security event log analysis tools, network traffic analysis tools, and specialized tools that detect certain image characteristics(like pornographic material), or text format characteristics(like Social Security or credit card numbers).
- *Reporting tools* – These facilitate tagging and reporting of evidence in various formats suitable for the incident response team, management, law enforcement, and others.
- *Workflow and documentation tools* – These track every step in the incident response process, from initial report through resolution. Some also facilitate collection and storage of documentation at each step, as well as provide historical data needed to generate incident-related metrics.

Incident response tools in these and other categories are generally available as single products, although they might also be included in integrated product suites that seek to provide incident responders with a common "workbench" of tools from multiple categories. Additionally, these tools might be featured in products having much broader purposes than simply incident response. For example, products that facilitate governance, risk, and compliance process, i.e., GRC systems, typically include an incident/issue workflow and documentation component.

See the Information Security Incident Management (ISO 16) chapter of the EDUCAUSE Information Security Guide for further training and tools guidance.

Additional Resources

- The Information Security Incident Management (ISO 16) chapter of the EDUCAUSE Information Security Guide provides an overview of effective incident management approaches, a list of recommended tools for incident handlers, links to example practices at selected institutions, and other helpful guidance.
- Special Publication 800-61: Computer Security Incident Handling Guide issued by the National Institute of Standards and Technology (NIST) provides guidelines on detecting and handling incidents.
- Special Publication 800-83: Guide to Malware Incident Prevention and Handling for Desktops and Laptops issued by NIST.
- Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response issued by NIST.
- DEBIX, Inc. developed and makes publicly available a "Data Breach Incident Response Workbook." Though this general guidance resource was written for the private sector, much of the content is applicable to Higher Education as well.

Download the Checklist

The Sensitive Data Exposure Incident Checklist is available to download in PDF or Word format. The 12-page checklist includes all five steps and sub-steps.

⚠️ *Note: You may also view the complete checklist in the next section; however, if you are planning to print the checklist, we recommend downloading the PDF or Word version.*

Sensitive Data Exposure Incident Checklist (*Version 1.0: April 2012*)

Incident # _____

Date became aware: _____

Date reported to Security Office: _____

Date affected individuals notified: _____ *(should be within one week of incident discovery*)

Type and scope of data exposed: _____

Incident Team: _____

STEP 1: Identification

Verify that an incident has actually occurred. This activity typically involves the Unit systems administrator and end user, but may also result from proactive incident detection work of the Security Office or central IT operations. If it is determined that an incident has occurred, inform appropriate authorities.

Task	*Owner*	*Guidance*	*Examples*	*Additional Resources*

1.1 Immediately contain and limit exposure:
• If electronic device has been compromised:
  ○ Do not access (do not logon) or alter compromised device
  ○ Do not power off the compromised device
  ○ Do unplug network cable (NOT power cable) from the compromised device
• Write down how the incident was detected and what actions have been taken so far. Provide as much specificity as possible, including dates, times, and impacted machines, applications, websites, etc.
	Unit			• New York University IT Security Information Breach Notification Procedure
				• University of Massachusetts-Amherst Incident Prevention and Response Procedures

1.2 Alert Security Office immediately.	Unit	Instructions for alerting the Security Office should include multiple contact methods. Instructions should also reference the institution's security incident reporting policy, if one exists.	• Call John Smith at 999-999-9999 or Mary Jones at 999-999-9999. If you do not get one of them IN PERSON, then call the Help Desk at 999-999-9999 and have them contact the Information Security Office. Also send details to it-incident@xxxxx.edu • Report incident via online form (preferred) or call John Smith at 999-999-9999	• Indiana University Incident Reporting Procedures • University of Virginia Information Security Incident Reporting Policy and online reporting form
1.3 If the incident involves electronic devices or media stolen or lost within the local community, also alert law enforcement.	Unit	This sub-step should be included ONLY if advised to do so by your campus police department. Be certain to consult with them on this issue.	• Call Campus Policy Hotline at 999-999-9999 • Call E-911 to report the incident. The E-911 service will contact the appropriate city, county, or campus police jurisdiction.	
1.4 Conduct preliminary assessment of type and scope of data exposed. If the incident potentially exposed sensitive data, notify all appropriate institution officials and keep them informed as incident investigation progresses.	Security Office		Institution officials to be contacted might, among other, include: • Executive in charge of IT for the institution, e.g., Vice President/CIO • Executive in charge of organizational unit in which incident occurred, e.g., Vice President, Provost, Dean • Campus Chancellor/President (or his/her Chief of Staff) • Counsel for the institution • Law enforcement, e.g., campus police, FBI local office, Secret Service local office • Public Affairs • Internal Audit • Risk Management • Appropriate Data Steward(s) for the type of data potentially at risk • Health information compliance office, if HIPAA-protected potentially at risk • Vice president for research, if research data potentially at risk • Finance office, if credit card #, bank account #, or other sensitive financial data potentially at risk	
1.5 If there is evidence of criminal activity connected with the incident, determine interest of law enforcement in leading the investigation. If law enforcement (e.g., FBI) takes lead, subsequent steps may be performed by law enforcement or require authorization from the law enforcement lead.	Security Office			

STEP 2: Damage Containment and Data Exposure Assessment

Identify an Incident Response Lead and assemble an incident response team charged with limiting further damage from the incident. Conduct a thorough assessment of the type and scope of data exposed following applicable laws, regulation and policy.

Task	Owner	Guidance	Examples	Additional Resources
2.1 Assemble Incident Response Team.	Security Office	Ensure that the representative from the organizational unit where the incident occurred participates and that this individual is high enough in the organization to make necessary decisions.		
2.2 Review incident response process and responsibilities with Incident Response Team. In particular: • Provide each member with current Sensitive Data Exposure Incident Checklist • Discuss communications strategy • Stress importance of maintaining chain of custody	Security Office	Discussing the rules of communication with the team at this stage is particularly important to ensure accuracy of facts among team members and between the team and appropriate University officials.	Rules of communication might, among other things, include: • Team members must not discuss the incident with anyone outside the team until and only if authorized to do so by the Security Office head. • All documentation created by team members must be fact-based, as it may become important reference or evidence • Daily conference call of team members will be held discuss status. • Instruct team to track time spent on the incident.	
2.3 Collect and preserve evidence.	Incident Response Team	Collect sufficient physical and cyber evidence to provide a clear, detailed description of how the sensitive data was compromised.	Evidence types include, but are not limited to: • Image of hard drive(s) physical equipment • Network traffic flow to/from compromised device • Workstation and application logs • Access logs • Digital photographs of the evidence and surrounding area	• http://www.educause.edu/Resources/ForensicOverview/161135 • http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf • http://csrc.nist.gov/publications/nistpubs/800-61-rev2/SP800-61rev2.pdf
2.4 Establish and maintain appropriate chain of custody for all evidence*.*	Incident Response Team	Inventory pieces of evidence and track who accessed, used, stored, moved or returned each piece of evidence and when it was accessed.	Good chain-of-custody practices include, but are not limited to: • Establishing what exactly the evidence is • Documenting who handled it and why • Documenting where and how it was stored • When equipment is moved, ensuring that a detailed receipt is signed and dated by the previous person with possession, the mover and the new person with responsibility for the equipment	• http://www.cert.org/csirts/services.html • http://www.sans.org/score/incidentforms/ChainOfCustody.pdf
2.5 Take actions needed to limit the scope and magnitude of the incident.				
Incident Response Team		Incident containment actions include, but are not limited to: • If the incident involves sensitive data improperly posted on one or more publicly accessible websites, remove active and cached content and request takedown of cached web page(s) indexed by search engine companies and other Internet archive entities, e.g., Wayback Machine • Change passwords that may have been compromised • Cease operation of a compromised application or server		
2.6 Perform forensics and document findings: • Analyze evidence • Reconstruct incident • Provide detailed documentation	Incident Response Team	• Preserve original evidence and work on a copy of data. • Conduct forensics with minimal disturbance to units, systems and original evidence. • Results should be repeatable.		http://www.nij.gov/pubs-sum/199408.htm
2.7 Complete final assessment and documentation of type and scope of data exposed, as well as the availability and type of contact data for individuals affected	Incident Response Team			

STEP 3: Eradication and Recovery
Take steps to remove the cause of the exposure, reduce the impact of the exposure of the sensitive data, restore operations if the incident compromised or otherwise put out of service a system or network, and ensure that future risk of exposure is mitigated.

Task	Owner	Guidance	Examples	Additional Resources
3.1 Revisit 2.5 and look for additional ways to limit exposure				
Incident Response Team		Additional ways to limit exposure include, but are not limited to: • Running web queries periodically to ensure that the data has not been further exposed or cached. • Reviewing the inventory of equipment and systems impacted and change additional passwords that may have been compromised • Ceasing operation of a compromised application or server and develop work-arounds		
3.2 Eradicate and/or mitigate system vulnerabilities, review access privileges and remediate risks to sensitive data stores				
Incident Response Team		Possible actions include, but are not limited to: • Run vulnerability scans on impacted systems; • Review and determine where data resides and make adjustments to ensure increased protection as needed. • Limit access to systems to only those who need it; • Use software tools to find, delete and secure sensitive data, e.g., Identity Finder		
3.3 Return evidentiary equipment and systems to service once they are secured.	Incident Response Team			

STEP 4: Notification

Determine the need to give notice to individuals whose data may have been exposed by the incident. Swiftness in notifying those affected by a breach of personally identifiable information, as well as informing certain government entities, is legally mandated in many states and, depending on the nature of the data, also federal law. Speed is also important from a public relations standpoint. To this end, many of the sub-steps can and should be undertaken in parallel to accommodate these needs.

Task	Owner	Guidance	Examples	Additional Resources

4.1 Make decisions based upon Incident Response Team findings
• Does level of exposure risk warrant notification letters?
• If yes,
  ◦ If applicable, has law enforcement authorized notification to affected parties?
  ◦ Who will issue letter?
  ◦ Who will handle telephone and email responses to questions from affected individuals? Does expected volume warrant setting up call center?
  ◦ Does magnitude of exposure warrant a press release? Incident information website?
  ◦ Does exposure risk warrant free credit monitoring?
• If a reasonable risk of exposure does not exist, all remaining sub-steps in this section should be bypassed and STEP 5 Follow-up should commence.
	Appropriate institution officials	• Those responsible for making these decisions will vary from institution to institution, but typically is a subset of officials informed in Sub-step 1.4. Decisions made should be in line with previous decisions or any deviations fully justified. Obviously, all relevant incident notification laws, regulations, and contractual requirements must be followed.
		• Opinions diverge on which state notification law(s) must be followed when individuals affected by the breach are citizens of states other than the state where the incident occurred. The advice of University Counsel should be sought on this matter.
		• While breach notification laws, regulations, and contractual requirements vary, alternatives to issuing written notices by postal mail are often allowable depending upon the cost of providing notice, the number of individuals who must be notified, and/or the availability of contact information. These alternatives might, for example, include, but are not limited to, one or more of the following: conspicuous posting of notices on the institution's website, press releases, email notices where addresses are known, telephone notices.
				EDUCAUSE Data Incident Notification Toolkit
				
				Determining Notification in Event of Breach

4.2 Collect name and contact information on affected individuals	Unit, advised by Security Office	This could be a laborious process if individuals are not current students, faculty, staff, donors, patients, etc. of the institution. It is advisable that the best sources of address data for former students, faculty, and staff, as well as alumni, volunteers, contractors, and other affiliates of the institutions whose sensitive data are maintained by the institutions be identified in advance, so that notifications can be made quickly in the event of data exposures. Ensure that data is collected, transmitted and stored securely and removed when it is no longer needed.		
4.3 Set up telephone and email support for affected individual questions: • Identify appropriate person(s) to handle calls and emails • Establish telephone call line/routing infrastructure, if not available • Identify/set up telephone number to use • Identify/set up email address to use • Train individuals handling calls and emails, including providing them with a list of anticipated questions and answers	Unit, advised by Security Office			EDUCAUSE Data Incident Notification Toolkit – Incident Response FAQ (Section Four)

4.4 If deemed appropriate by institution officials in Sub-step 4.1, create website for affected individuals
• Identify URL and location
• Restrict access until ready to go live
• Draft content
	Unit, advised by Security Office	• Incident websites are typically reserved for situations in which contact information for individuals affected by the breach is unknown or incomplete.
		• Website content should be approved by appropriate institution officials, e.g.,
		  ◦ Executive in charge of IT for the institution, e.g., Vice President & CIO
		  ◦ Executive in charge of organization in which incident occurred
		  ◦ Public affairs office
		  ◦ Counsel for the institution
				EDUCAUSE Data Incident Notification Toolkit – Incident-Specific Web Site Template (Section Three)

4.5 If deemed appropriate by institution officials in Sub-step 4.1, obtain free credit monitoring services for affected individuals	Unit, advised by Budget and Purchasing Offices	Obtain clear instructions to provide affected individuals signing up for free credit monitoring services and include this information in notification letters, websites, and email/telephone support FAQs.		

4.6 If deemed appropriate by institution officials in Sub-step 4.1, prepare press release
• Identify contact for media
• Compose text for press release
• Develop talking points
	Public Affairs	• Press releases are often reserved for situations in which contact information for individuals affected by the breach is unknown or incomplete, but it's wise to have a pre-approved media statement in hand to use in addressing media inquiries.
		• Content should be approved by appropriate institution officials, e.g.,
		  ◦ Executive in charge of IT for the institution, e.g., Vice President & CIO
		  ◦ Executive in charge of organization in which incident occurred
		  ◦ Public affairs office
		  ◦ Counsel for the institution
				EDUCAUSE Data Incident Notification Toolkit – Building a Press Release (Section One)

4.7 Prepare notification letter to affected individuals • Identify letter issuer and letterhead to be used • Compose draft text	Unit, advised by Security Office	Letter content should be approved by appropriate institution officials, e.g., • Executive in charge of IT for the institution, e.g., Vice President & CIO • Executive in charge of organization in which incident occurred • Public affairs office • Counsel for the institution		EDUCAUSE Data Incident Notification Toolkit – Notification Letter Components (Section Two) http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html FERPA: http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html Other data protection laws, http://protect.iu.edu/cybersecurity/data/laws
4.11 Notify granting organizations and research partners if research data compromised, as dictated by contractual obligations	University Counsel or designated office			
4.12 Notify appropriate third-party service providers for the institution if doing so would reduce the risk of identity theft for affected individuals or dictated by contracts.				
Unit		Appropriate third-party service providers might include, but are not limited to: • Employee benefit vendors • Student services vendors		
4.13 If Credit Card data exposed, notify the credit card processor(s) or merchant banks	Treasurer	Specific notification requirements are governed by the card brand.	VISA: http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html	
4.14 Notify Credit Bureaus as required by State and upon consultation with University Council	Treasurer with advice from University Counsel			
4.15 Coordinate simultaneous mailing of letters to affected individuals, issuance of press release if applicable, activation of website if applicable, notifications to regulatory entities and third-party vendors.	Unit, Security Office, University Counsel, and Public Affairs			
4.16 Ensure that notification of the data breach is added to the record of access to the affected individuals file as required by Federal or State law.	Data Custodian			

STEP 5: Follow-up
Identity lessons learned from the incident, implement any remediation needs, and securely store a complete record of the incident.

Task	***Owner***	***Guidance***	***Examples***	***Additional Resources***
5.1 Collect staff time spent during event and record in the incident documentation (especially for those cases that might be prosecuted)	Unit gathers data from all affected parties and provides to Security Office			
5.2 Schedule a debriefing meeting two to six weeks afterwards to review what could have been done better in responding to the incident.	Security Office, Public Affairs, University Counsel, and appropriate others			
5.3 Assess remediation needs • Issue report to unit manager and executive management if appropriate • Follow up to ensure completed				

Security Office		Issues for consideration include, but are not limited to: • Why was the data stored in a vulnerable place? • What more could have been done to avoid the intrusion? • Is the unit taking appropriate steps to remediate?		
5.4 Initiate plans and projects to implement remediation needs. • Apply lessons learned and recommended changes to access, sensitive data stores, systems and processes to increase protection	Unit			
5.5 Securely file all records, communications, notes, and other incident artifacts. Retain and eventually securely destroy this incident information in accordance with established records retention policies and schedules.				
Security Office				

Questions or comments? Contact us.