Incident Response FAQ (Section Four)

Other Toolkit Sections

Toolkit Home | Section 1: Building a Press Release | Section 2: Notification Letter Components | Section 3: Incident-Specific Web Site Template | Section 5: Generic Identity Theft Web Site

Introduction

This template can be used to guide development of "frequently asked questions" information to include as part of a notification letter, website or other materials concerning a specific security incident. Answers to questions in this template are *examples only*. They need to be adjusted for the unique circumstances of the incident.

Individuals potentially affected by an incident will have varying levels of computing knowledge - possibly none. It is, therefore, critical that explanations of the incident, the potential for impact on them, and steps they should take, if any, be communicated in clear and concise terms. Institutions should carefully consider the specific information these individuals will want to know and address only those issues. Explanations should be short, to the point, and free of technical jargon.

If a hotline is setup, the institution will need a mechanism for gathering the questions and answers being provided via the hotline so the online FAQ is updated frequently and appropriately.

Question: I received a notification via e-mail/letter from (institution name) about a computer security incident. Does that mean someone stole my personal information?

Example Answer: No. The (institution name)'s investigation into this incident revealed that an unauthorized person gained control of a computer containing a confidential file. It is possible the intruder's intent was to either disrupt normal business or use the computer's processing power to launch similar attacks on other computers. He or she may not have been aware the confidential file was stored on this computer. We do not have sufficient evidence, however, that the file was not acquired. The (institution name) has, therefore, taken the precautionary measure of distributing an advisory to all individuals whose information was in the file, so that they can take appropriate steps if concerned. Thus far, there have been no reports of unauthorized use of personal information as a result of this computer security breach.

Question: What personal information was involved? When was it available to the unauthorized person? And for how long?

Example Answer: The confidential file contained names, addresses, birth dates, and social security numbers of individuals who submitted applications for admission to the (institution name/school) in 2004. Current information indicates the unauthorized person gained control of the computer from September 1, 2005 to September 8, 2005.

Question: Is this information still at risk of disclosure to an unauthorized person?

Example Answer: The computer involved in this incident has been secured. The (institution name) is taking precautions to minimize future security risks.

Question. What should I do if I discover fraudulent use of my personal information?

Example Answer: Individuals whose personal information was involved in this incident can request a free initial (90 day) fraud alert to be placed on their credit files by calling any one of the three major national credit bureaus or completing an online form. Submit one online form request and all three agencies will add the fraud alert.

- Equifax
  Direct Line for reporting suspected fraud: 800-525-6285
  Fraud Division
  P.O. Box 740250
  Atlanta, GA 30374}
  800-685-1111 / 888-766-0008
  http://www.equifax.com

- Experian
  Direct Line for reporting suspected fraud: 888-397-3742
  Credit Fraud Center
  P.O. Box 1017
  Allen, TX 75013
  888-EXPERIAN (888-397-3742)
  http://www.experian.com

- Trans Union
  Direct Line for reporting suspected fraud: 800-680-7289
  Fraud Victim Assistance Department
  P.O. Box 6790
  Fullerton, CA 92634
  Phone: 800-916-8800 / 800-680-7289
  http://www.transunion.com

When contacting the Credit Reporting Agency, you should request the following:

1. Instruct them to flag your file with a fraud alert including a statement that creditors should get your permission before opening any new accounts in your name.

2. Ask them for copies of your credit report(s). (**Credit bureaus must give you a free copy of your report if it is inaccurate because of suspected fraud.**) Review your reports carefully to make sure no additional fraudulent accounts have been opened in your name or unauthorized changes made to your existing accounts. **NOTE:** In order to ensure that you are issued free credit reports, we strongly encourage you to contact the agency's **DIRECT LINE (listed above) for reporting fraud**. We do not recommend that you order your credit report online.

3. You may want to ask about the option to freeze your credit. Forty-seven states and the District of Columbia have enacted legislation allowing consumers to place "security freeze" on their credit reports. A consumer report security freezes limits a consumer reporting agency from releasing a credit report or any information from the report without authorization from the consumer. Check your state's information.
4. Be diligent in following up on your accounts. In the months following an incident, order new copies of your reports to verify your corrections and changes, and to make sure no new fraudulent activity has occurred.
5. If you find that any accounts have been tampered with or opened fraudulently, close them immediately. To ensure that you do not become responsible for any debts or charges, use the ID Theft Affidavit Form developed by the Federal Trade Commission to help make your case with creditors.

You may request a free annual credit report, 1 per year, from AnnualCreditReport.com as recommended by the Federal Trade Commission.

Question: Will (institution name) contact me to ask for private information because of this event?

Example Answer: In similar cases at other institutions, people have reportedly been contacted by individuals claiming to represent the University and who then proceed to ask for personal information, including social security numbers and/or credit card information. Please be aware that (institution name) will only contact you about this incident if additional helpful information becomes available. We will not ask for your full Social Security number. We will not ask for credit card or bank information. We recommend that you do not release personal information in response to any contacts of this nature that you have not initiated.

Question: Who should I contact if I have any additional questions concerning this security breach?

Example Answer: In order to answer any questions that you may have regarding this incident a special phone line, (xxx) xxx-xxxx (toll free 1-888-xxx-xxxx), has been activated and will be monitored by the (institution's name).

Questions or comments? Contact us.