Building a Press Release (Section One)

Other Toolkit Sections

Toolkit Home | Section 2: Notification Letter Components | Section 3: Incident-Specific Web Site Template | Section 4: Incident Response FAQ | Section 5: Generic Identity Theft Web Site

I. Before getting started

A. Do I need to issue a press release?

B. Who will the press release be sent to? Victims? Media outlets?

C. What medium will be used for the press release?

D. Do I have legal obligations relative to the press release? Is it serving as "substitute notice" per state law?

II. Elements of a press release

A. Summary statement

i. The first sentence of a news release should contain a summary of the entire story so that those reading the release know exactly what is going on.

ii.What are you doing?

- Announcing a breach? A theft?
- Announcing that the case has been resolved? That notification has occurred?

C. Brief incident details:

ii. Who is affected/not affected? What specific types of personal information are involved?

iv. What does evidence suggest? (e.g. "No evidence to indicate data has been misused...")

D. Expression of regret (if appropriate)

i. If details of the incident are still unclear, it may not be appropriate or advisable to express regret.

E. Concrete steps the institution is taking to prevent this from happening again.

F. Major (re)actions taken.

G. For more information, ...

III. Sample snippets

A. Introduction and Basic Description

1. University of Kansas officials today announced they have detected suspected computer hacking into a file server that contained records on 1,450 students, most of whom were international students.

2. University of California, Berkeley, police are investigating the theft of a campus laptop computer that contained files with the names and Social Security numbers of more than 98,000 individuals, mostly graduate students or applicants to the campus's graduate programs.

3. UCLA began mailing letters June 5 about the theft of a laptop computer from a locked van at a UCLA blood drive last November. The computer held a database containing personal information from some 145,000 people who have donated blood and platelets to the UCLA Blood and Platelet Center since 1985.

4. A Boston College student has been suspended from the University for violation of the University's computer use policy after he admitted to illegally obtaining personal identification numbers (PIN) and Social Security numbers of a number of BC students, staff, faculty and recent graduates by using keystroke-capturing software.

B. Impacted Persons and the Information at Risk

5. The server contained personal information, including names and Social Security numbers, on current, former and prospective students, as well as current and former faculty and staff.

6. The stolen computer contained information on most individuals who applied to graduate school at UC Berkeley between fall 2001 and spring 2004 (except law school students in the JD, LLM, and JSD programs); graduate students who registered at UC Berkeley between fall 1989 and fall 2003 (including law school students in the JD, LLM, and JSD programs); recipients of doctoral degrees from 1976 through 1999 (excluding law school students in the JD program); and other small groups of individuals. Approximately one-third of all of the computer's files contained dates of birth and/or addresses in addition to Social Security numbers and names.

7. The server contained personal information, including names and Social Security numbers, on current, former and prospective students, as well as current and former faculty and staff. The vast majority of students involved were new students within the past five years. The faculty and staff data was contained in a file from the Wildcat Card identification system.

8. The server did not include any information related to the UConn Health Center's electronic patient records and no patient information was affected, said Kerntke.

9. Student laptop computers were not breached, and, at this time, school officials believe that [population e.g. current undergraduates] were not affected.

C. Incident details

10. Five apparent hacking incidents, which took place between Jan. 6 and 17, were discovered Jan. 21. Once officials determined yesterday that university data had been downloaded, the incidents were reported immediately to the Federal Bureau of Investigation, the INS and other appropriate agencies. The university is assisting the FBI in efforts to identify and apprehend the person or people responsible for the hacking.

11. The University discovered the hacking during routine monitoring of the network. An investigation revealed that the hackers installed software to store files, such as for movies or games, on the system and attempted to break into other computers.

12. The computer was stolen March 11 when an individual entered a restricted area of the Graduate Division offices that was momentarily unoccupied. A campus employee saw the individual leaving with the laptop and contacted campus police. The case remains under investigation.

13. According to Moore, an extensive computer forensics investigation concluded that the computer was not targeted to access personal information, but to allow the hacker to launch attacks on other computers on the Internet.

14. As a result of the detection, the computer was immediately taken off-line and the breach secured.

D. "Statements of Perceived Risk"

15. "Even though we believe this incident puts users of University technology at low risk of identity theft, we felt it was essential to notify them of the incident," he said. Kerntke advised individuals to consider submitting a fraud alert to the three national credit reporting agencies as this will make it more difficult for identity theft to occur.

16. "While this is worrisome, we have no evidence that anyone has extracted the private information and is using it," she added. "We wanted to advise our donors to be extra alert to signs of possible misuse of their personal identities."

17. In a statement to the media, Director of Public Affairs Jack Dunn said there was no evidence that personal information was accessed in any way, but given the seriousness of the issue, Boston College decided to send out a precautionary advisory to those alumni whose names were on the database with Federal Trade Commission guidelines they could follow to help ensure their privacy.

18. "Based on forensic analysis, there is no indication that any of the data on the machine was actually compromised---only that the opportunity for someone to access it existed," Kerntke said. "Even so, the University wants to be sure individuals are aware of the situation so they can carefully monitor their financial records for unauthorized activity over the next several months."

19. The student, whose identity is protected under student privacy laws, admitted to the dean of student development that he had gathered the information by exploiting a security hole in Microsoft Windows on several public computers on campus, but denied having divulged the information externally in any way. An investigation by the Boston College Police Department confirmed that the information was not misused externally.

20. "Even though we believe this incident puts users of University technology at low risk of identity theft, we felt it was essential to notify them of the incident," he said.

21. No evidence of unauthorized use of personal information included on the computer system has been discovered. However, potential risks associated with identity theft are serious, and the school's administration has taken precautionary steps to inform all affected students, graduate alumni, faculty, staff and others whose information may have been contained on the system about safeguarding measures aimed at protecting privacy.

22. The University reports that it has no evidence that personal information was accessed in any way. However, given the seriousness of the issue, Boston College decided to send out a precautionary advisory to those alumni whose names were on the database. The advisory includes FTC Guidelines to help guard against identity theft.

E. Apology or statement of commitment to security

NOTE: Apologizing for an incident could serve as an admission of guilt and create unnecessary risk to your institution, especially in situations where litigation might follow. Such a statement should be reviewed by General Counsel and Public Relations to ensure the institution is in agreement on whether or not an apology is appropriate. This is especially important if an incident is still under investigation.

23. "We deeply regret this situation and are taking steps to support the affected students," said Provost and Executive Vice Chancellor David Shulenburger. "We will help them in every way possible and do our best to protect against future intrusions."

24. "We deeply regret our delay and the security breach," she said. "We have put new measures into place to better assure that sensitive data stored on laptops are encrypted, protected and limited to essential need."

25. "Blood donors are generous people who sustain the lives of thousands of UCLA patients each year. We would feel terrible if any harm befell them," said Dr. Priscilla Figueroa, director of transfusion medicine for UCLA Medical Center.

F. Major (re)actions taken to prevent future occurrences

26. "We are doing everything we can to prevent this from happening again in the future," he said, noting that the University is reviewing its dependence on social security numbers as a unique identifier, auditing other servers and departments that are not directly part of the breached system but contain or transmit sensitive information, and implementing even more stringent network and server access controls while striving to support the technologically collaborative environment essential to a comprehensive research institution like UConn.

27. Social Security numbers will display only the last 4 digits wherever possible. Helpdesk staff will assist UCLA Healthcare employees in removing private information from laptop and desktop computers and relocating it on secure network servers. Employees must encrypt any sensitive information that needs to remain on their computer's local drive.

28. Upon learning of the breach, Executive Vice President Patrick J. Keating organized a task force of staff from Information Technology, Human Resources, Student Services, Student Affairs, BCPD and Public Affairs, along with a consultant from the Massachusetts State Police, to address the issue.

G. Major (re)actions taken to limit impact to victims

29. "The university will provide anybody whose information was on the hard drive with free identity theft insurance for one year," he said.

30. "The university is offering to pay for consumer identify theft protection insurance for all involved. At a negotiated rate of $7 per person, the total cost will be about $42,210."

31. "We have arranged for you to sign up for a one-year credit protection program from ConsumerInfo.com, Inc., an Experian®, at no cost to you. This program includes identity theft insurance."

H. For more information

32. The School will provide updates for its constituents via the Internet. A Web site providing information and frequently asked questions can be found at <URL>. Affected individuals also can call 1-800 for more information or send an e-mail to school-incident@school.edu.

33. In addition, the University has established an alumni phone line at (866)683-6369 that will be staffed by BC employees to answer questions regarding the breach. Information is also available at http://www.bc.edu/offices/techsupport/security/.

34.Keating suggested that any faculty and staff with questions on this issue should contact the Office of Human Resources at ext.2-3330. Students should contact Student Services at ext.2-8900.

Questions or comments? Contact us.

Except where otherwise noted, this work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0).