Incident Response Plan

The Importance of Securing Electronic Data

Much of the data stored or transmitted via Whitman's computing equipment is confidential. Unauthorized access to this data may constitute a violation of federal statutes such as the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Graham-Leach-Bliley Act (GLB), and other laws designed to protect privacy. A breach in data security that compromises personal information can lead to identity theft, putting members of the Whitman community at risk and exposing the College to litigation. Unauthorized access to other confidential data, though not usable for identity theft, may nonetheless have serious legal, financial, or public relations implications for the College.

Preventing Electronic Data Breaches

The task of protecting confidential electronic data is shared by all members of the Whitman community who have authorized access to such data. In general, confidential data should not be accessed, copied, stored, downloaded, transmitted, or used unless it is essential to do so to conduct College business.

Confidential data should not be stored on laptops or other mobile devices for longer than necessary and should be encrypted at all times when not actually in use. Devices that contain confidential data, whether mobile or not, should be secured by strong authentication (e.g., multiple levels of passwords) as well as by physical means (security cables, locked cabinets, etc.). Mobile devices should not be put into checked luggage when traveling.

The Chain of Responsibility

Under certain circumstances, confidential electronic data — such as student names, email addresses, or other information — may need to be conveyed to individuals or groups who are not employees of the College. These may be vendors, contractors, professional organizations, (internal) student organizations, or others. In these circumstances, the College must require the recipient of the data to abide by the same (or stricter) guidelines to protect the data from unauthorized access or abuse. This chain of responsibility must extend to any third parties (or beyond) to whom the confidential data might be further conveyed.

Responding to Data Security Breaches

Despite explicit guidelines for securing confidential electronic data, breaches can still occur. At such times, it is important that the College respond as quickly and as professionally as possible. Computer thefts, should be reported immediately to Office of Information Technology (ext. 5415 or 509-527-5415). Steps that Office of Information Technology will take in the event of a data security breach are as follows:

1. Determination of the nature and scope of a breach

- identification of the person reporting the breach (name, contact info, etc.)
- record of the location, timeframe, and apparent cause of the breach
- preliminary identification of confidential data that may be at risk

2. Communication about breach to authorized individuals

- chief information officer
- director of security (if physical entry or hardware are involved)
- president and senior officers (depending on severity of data compromised)
- law enforcement (depending on the nature/magnitude of theft)
- legal counsel (depending on severity of data compromised)

3. Investigation of breach

- confirmation/inventory of confidential materials at risk
- security measures that were defeated or circumvented
- forensic evidence
- likelihood of recovering data (or stolen equipment)
- utilize outside assistance if needed

4. Assessment of breach

- password changes and other security measures to prevent further breaches
- identify individuals affected by the breach (e.g., those whose loss of confidential information may put them at risk of identity theft or other adverse consequences)

5. Remediation

- determine if lost data can be restored from backups; take appropriate steps
- determine if lost data can be neutralized by changing account access, ID information, and taking other steps

6. Notification of breach - senior officers and CIO will determine need and method(s) to:

- notify affected individuals

- notify Whitman community
- notify public

Guidelines for Community and Public Notifications

If senior officers and the CIO determine that community and/or public notifications are indicated, the president—or a person designated by the president to serve as spokesperson—will convey information and answer questions about the incident. Others should refer all questions to the president or designated spokesperson.

Communications will cover the following points:

- nature and scope of missing data (e.g., alumni contact information, etc.)
- general circumstances of the breach (e.g., stolen laptop, hacked database etc.)
- rough timeline of the breach (e.g., date)
- steps the college has taken to investigate and assess the breach
- involvement of law enforcement or other third parties
- knowledge of any misuse of the missing data
- steps that affected individuals may wish to take
- steps that the college is taking to prevent future breaches of this nature

Post-Incident Follow-Up

In the wake of a serious data security breach, Office of Information Technology will:

- insure that missing data (e.g., passwords) cannot be used to access further information or cause harm in other ways to Whitman's electronic or other resources;
- pursue all reasonable means to recover the lost data
- modify procedures, software, equipment, etc., as needed to prevent future data breaches of a similar nature;
- take appropriate actions if personnel negligence caused or contributed to the incident.

Adapted with permission from Reed College Computing & Information Services http://web.reed.edu/cis/policies/incident_response.html

Related articles

- Encryption
- Encrypting Folders and Files on Mac
- Encrypting Folders and Files on Windows
- Cloud Storage Guidelines
- Secure File Exchange