Data Breach Guidelines

A system-wide guide and procedures to reacting to suspected and actual data breaches

FINAL

Danny Miller, C|CISO, CISA, CRISC, CGEIT, ITIL
System Chief Information Security Officer - TAMUS

Definition of Data Breach

A data breach is an incident in which sensitive, protected, or confidential data has **potentially** been viewed, stolen or used by an individual unauthorized to do so.

No single federal law or regulation governs the security of all types of sensitive information. "Sensitive information" could include:

- Protected Health Information/ HIPAA
- PII - Social Security Numbers/ Bank Account Records
- Credit Card Numbers
- Others:
  - ✓Student information?
  - ✓Intellectual Property?

What happens in a data breach?

- In most organizations, breach notification will come from an external entity. Very few organizations have the required detective controls in place to know if data was read/copied by an unauthorized party.
- How do they know it's you? Determination of **"Common point of purchase"**
- **Forensic analysis** – Determining the extent of the losses
- **Compliance status** – Determining the compliance of organizations with applicable laws / regulations
- **Remediation** – Implementation of controls to prevent reoccurrence
- **Monitoring** – Continuous process of evaluating the effectiveness of those implemented controls.
- **Follow up / Fines** – Depends upon the severity of the breach, and "willful non-compliance"

What do we have to do?

- Covered entities under HIPAA's breach notification rule are required to develop a remediation plan for breaches to understand what happened, assure proper steps are taken to prevent a reoccurrence, and notify government officials and impacted patients.

- State breach notification laws (now in 46 states, DC, PR, and USVI) generally require notification of individuals if their “personal information” was, or is reasonably believed to have been, acquired by an unauthorized person.

✓ **Have a breach incident response plan**

✓ **Communicate, communicate, communicate**

Critical timing windows for notification

- We must notify affected individuals “without unreasonable delay” after breach is discovered, and if the breach is HIPAA related, no later than 60 days

- May delay notification **if** law enforcement provides documented statement that notice would harm national security or impede criminal investigation

When is a breach "discovered"?

- "Discovery" means first day breach is known, **or reasonably should have been known**, to any employee, officer, or agent of company

- Knowledge of breach by **any employee** can trigger notification deadlines for TAMUS and its members

- The System should have in place:
  - Reasonable systems for detecting breach
  - Mechanisms to ensure that any employee who discovers breach reports to management or leadership

When is it not a breach?

- If de-identified information is disclosed
- If you believe, in good faith, that the unauthorized person could not reasonably have retained information
- If an employee accesses sensitive information without permission but in good faith, as long as there is no further unauthorized action
- If an employee reveals sensitive information to an unauthorized colleague, as long as there is no further unauthorized action

Obligations & Consequences

FERPA related – Notification must be made to all *students* whose information was potentially compromised. ITRM [IT policy] can help the department determine if notification is required and can provide suggested templates.

CONSULTATION WITH THE REGISTRAR IS REQUIRED (ITpolicy can help with this also).

BE AWARE: FERPA provides for a complaint procedure to the United States Department of Education with an ultimate sanction of withholding federal funds. While there is generally no private cause of action directly under FERPA, students can seek to hold the University or individuals liable under other statutes or common law tort theories. Faculty, staff, administration or students who violate the University's FERPA policy may be subject to corrective or disciplinary action, depending on the individual circumstances (reference http://www.oar.tamu.edu/oarwww/Registrar/General/FERPA.aspx) .

Obligations & Consequences (cont'd)

Failure to adequately protect confidential information can result in consequences defined by Texas Government Code - Distribution or Misuse of Confidential Information, Section 552.352

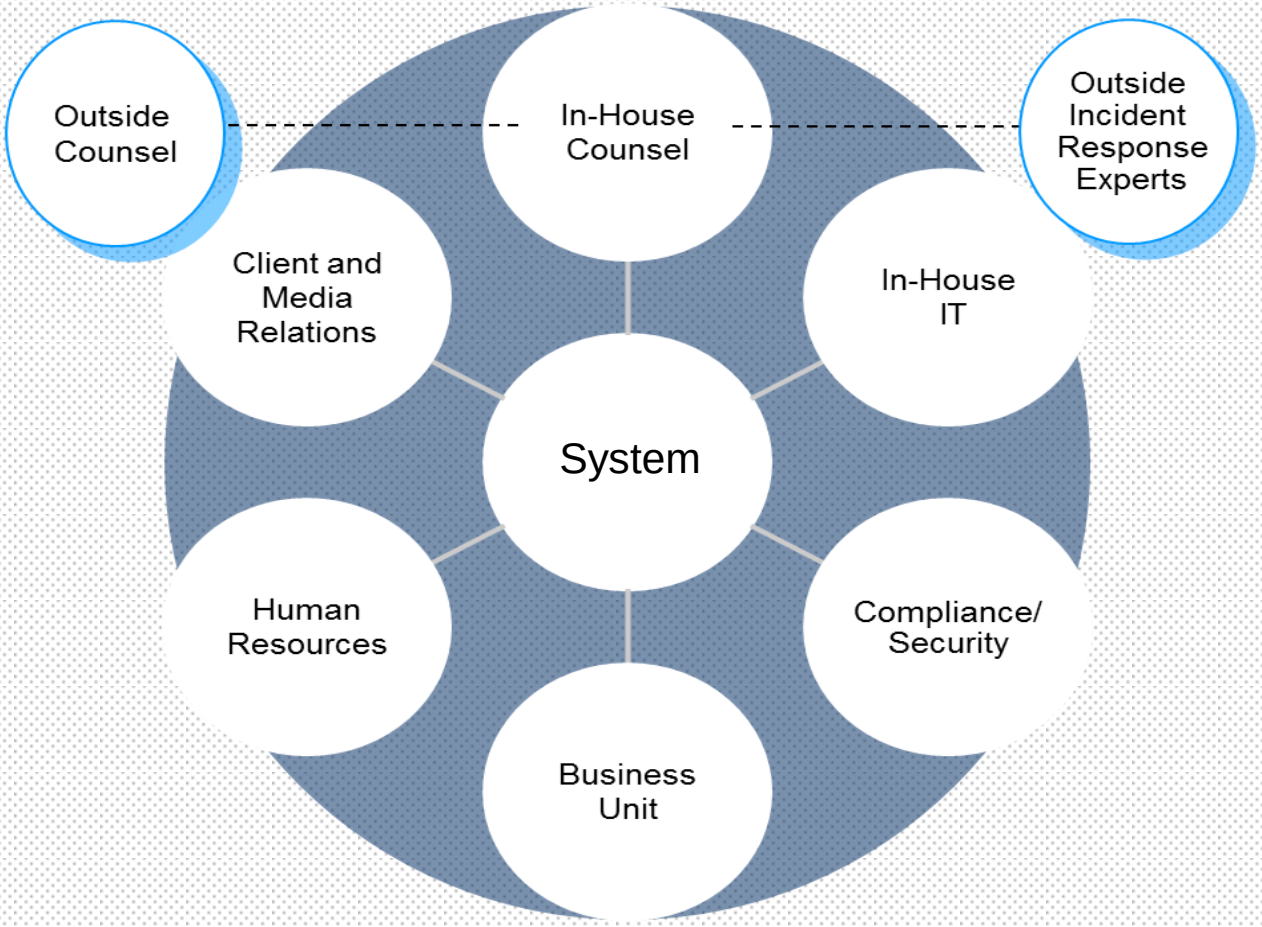
(1) a fine of not more than $1,000;
(2) confinement in the county jail for not more than six months; or
(3) both the fine and confinement.

NOTE: A violation under this section constitutes official misconduct.

Whom to notify

- Individuals whose information is believed to have been accessed, acquired, used or disclosed without authorization
  - Notify next of kin or personal representative, if affected individual known to be deceased
- Texas Attorney General of breach and with sample notification letter
- HIPAA / HITECH: Secretary of Health and Human Services
- PCI: Your payment processor/ back and the credit card brands, card holders
- Media notice, if cost to notify individuals would be beyond $250,000 or over 500,000 individuals would be required to be notified.

Team that needs to get involved in data breach



Procedures for a data breach

Once unauthorized disclosure, access, or use has been discovered, appropriate measures must be taken to halt any further unauthorized activity but preserve evidence for future analysis (take down the site, remove accessible documents if necessary, etc).

Keep in mind that mass email cannot be withdrawn. Follow typical incident management processes – identify, contain, eradicate, recover, follow-up.

1. Report the incident immediately: Danny Miller at 409.600.1614 or gdmiller@tamus.edu or SO-HELPME@tamus.edu.
2. IT Security may be able to help stop any breaches at the firewall and provide other forensic assistance. ITRM can help a department determine if 'notification' is required. If so, SOHELPME can walk a department through the notification process (reference SAP 29.01.99.M1.24 http://assets.system.tamus.edu/ITRules/29.01.99.S1.24.pdf).
3. Security@tamus.edu can help devise solutions to ensure similar breaches do not recur. SOHELPME will work with all appropriate System personnel and offices, including law enforcement, to ensure all required notification information is identified; and, can help ensure that all persons whose information may have been subject to unauthorized access, use, or disclosure are notified in accordance with applicable procedures and regulations.

Call List for Texas A&M University System

- Danny Miller, CISO of the Texas A&M University System
- Mark Stone, CIO of the Texas A&M University System
- Melia Jones, Office of General Counsel, Texas A&M University System
- Kevin McGinnis, Risk Management, Texas A&M University System
- Local Information Security Officer – Cary Tschirhart for TAMUS and see your Information Security Officer for issues at your location.

Documentation Requirements

The following information should be documented to help the department, IT Security, and Risk Management properly respond to incidents and complete required procedures:

Draft a brief summary stating what happened - a one or two sentence summary of how the information was lost, stolen, or otherwise exposed (e.g., a web page defacement or other internet exposure). Include the following details:

- when the breach occurred and/or when was it detected
- how the breach was detected - Did a student notify the department, did an employee notify the department, etc.
- a brief description of the data that was potentially compromised
- a brief description of measures that will be implemented to ensure similar situations don't recur

Reference Resources

RESOURCES:

FERPA - http://registrar.tamu.edu/general/ferpa.aspx
Texas Business and Commerce Code 521 Identity Theft http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.521.htm
System Data Security Guide https://apps.system.tamus.edu/datasecurity/index.html
TAMU Security Web page - http://security.tamu.edu/
SAPS – *Incident Management* and *Notification of Unauthorized Access*
Incident Management (currently under review with significant revisions)
http://rules.tamu.edu/PDFs/29.01.03.M1.09.pdf

Notification of Unauthorized Access, Use, or Disclosure of SPI
http://rules.tamu.edu/PDFs/29.01.03.M1.24.pdf

Contact Danny Miller for questions at 409.600.1614
or
gdmiller@tamus.edu