2009

Management of Data Breach

EDPS and ENISA,
Brussels

Bridget C. Treacy
Partner, Hunton & Williams
+44 (0) 20 7220 5731
btreacy@hunton.com
www.huntonprivacyblog.com

23 October 2009

HUNTON& WILLIAMS

HUNTON& WILLIAMS

Crisis Management

Key Objectives
▪Contain breach ▪Evaluate Risks Associated with Breach ▪Minimise risk of harm ▪Prevent recurrence

Co-ordinate Incident Response Team
▪Keep circle small ▪Involve key individuals (IS, legal, PR) ▪Assign specific tasks ▪Reference pre-agreed action plan ▪Regular updates

Conduct investigation to determine facts
▪Determine what data are involved ▪Establish cause and extent of breach ▪Determine who is affected by breach ▪Consider whether harm is likely to follow CONTAIN BREACH ASAP AND PRESERVE EVIDENCE

HUNTON& WILLIAMS

Key Decisions: internal v outside resources?

- Experience matters: use outside experts where internal experience is lacking
- Will need some immediate external assistance:
  - Forensic investigators and fraud specialists to
    - identify source of breach and contain it,
    - preserve digital evidence,
    - ensure independent and impartial investigation
  - Legal advice and co-ordination role, privilege

HUNTON& WILLIAMS

Key Decisions: who to tell and when?

- These decisions presume knowledge of the facts!!
- Consider whether and when to involve police
- Obligation to notify regulators and individuals depends on
  - Where individual based?
  - Where controller based?
- Local requirements vary
  - eg UK not mandatory but expected
  - May be harm-based test, or not
  - Exemptions eg encryption
- Whose data? Eg if vendor, notify customer (controller) and otherwise comply with contractual requirements
- Notify insurers? Card processors? Others?
- Manage notice to the world (prospective customers)

HUNTON& WILLIAMS

Preparing the Notification Letter

- Letters must be written with several readers in mind, including impacted individuals, regulators, the general public, the media and employees.
- If you notify in one jurisdiction, notify in all jurisdictions (which requires consideration of overseas notification standards)
- Use plain language
- Describe:
  - Personal information involved
  - Steps taken to protect against further unauthorised access / loss
  - How company will assist affected individuals
  - Guidance on how individuals can protect themselves from identity theft or fraud
  - Jurisdiction-specific information

HUNTON& WILLIAMS

Expected Offerings

- Notification letters to affected individuals generally contain a number of standard “offerings”
  - Instructions to close bank accounts or cancel credit cards, if necessary
  - Availability of free credit reports
  - Offer of an identity protection solution such as credit monitoring
  - Ability to place a fraud alert or security freeze in credit file
  - Reference to relevant website eg CIFAS, FTC

HUNTON& WILLIAMS

Pre-mailing Plan

- Need detailed pre-mailing plan of action
  - Prepare media release or holding statement
    - Involve PR team or communications group
  - Set up call centre or helpline
    - Prepare scripts/FAQs
    - Conduct training
    - Monitor initial calls
  - Draft website materials
  - Set up identity protection / credit monitoring arrangements
  - Consider investor relations
- Keep circle small

HUNTON& WILLIAMS

Avoiding Private Lawsuits

- Understand the scope of the breach before announcing it
- Finalise plan of action in advance of the announcement
- Don’t skimp on use of expert third parties (forensic investigators, lawyers, fraud specialists, PR firms)
- Be transparent, generous and helpful
  - to affected individuals and to the regulators

HUNTON& WILLIAMS

Lessons Learned

- Reputation is everything
- A small breach has a silver lining
- Have an incident response plan and team in place
  - be proactive, not reactive
- Involve senior management in data security – alert them to the multiple and varied risks
- Don't skimp on IS (budget or people)
- Attacks are more sophisticated than ever
- Re-evaluate security systems and policies on an ongoing basis
- Integrate the concern for information security as a core value and increase employee awareness

HUNTON& WILLIAMS

PRIVACY AND INFORMATION SECURITY LAW BLOG

GLOBAL PRIVACY AND INFORMATION SECURITY LAW UPDATES AND ANALYSIS

Stimulus Package Includes Breach Notice Obligations and Substantial Changes to HIPAA

POSTED ON FEBRUARY 2, 2009 BY HUNTON & WILLIAMS LLP

Provisions of the economic stimulus legislation (known as the American Recovery and Reinvestment Act ("ARRA")), recently passed by the U.S. House of Representatives, require certain entities to notify affected individuals, government agencies and the media of breaches of "unsecured protected health information." Additional provisions substantially revise regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). While these provisions are specifically limited to the context of health data, they have far-reaching implications for businesses across industry that manage personal information. Read more...

Email This
Print
Comments
Trackbacks

TAGS: ARRA, Articles, Breach, HIPAA, Stimulus legislation

HUNTON& WILLIAMS

Questions?

Bridget C. Treacy
Partner
Hunton & Williams
+44 (0) 20 7220 5731
btreacy@hunton.com