


SCCE's 7th Annual
Compliance & Ethics Institute

September 14–17, 2008
 Sheraton Chicago Hotel & Towers
 Chicago, IL


Responding to a Data Breach

Orrie Dinstein
 Chief Privacy Leader and
 Senior Counsel - IT & IP
GE Commercial Finance

Society of Corporate Compliance and Ethics
 6500 Barrie Road, Suite 250, Minneapolis, MN 55435, United States
 www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977





**SOCIETY OF CORPORATE
 COMPLIANCE AND ETHICS**



Data Losses are a global, industry-wide problem

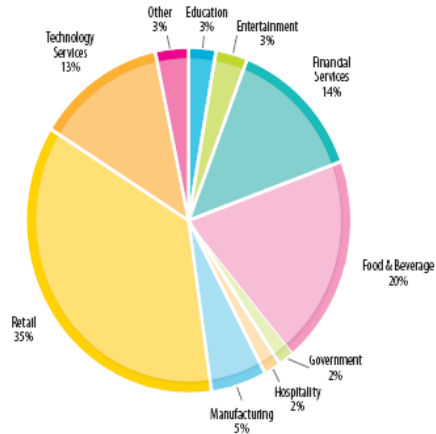
Year	Approx # of incident	# of people impacted (rounded to nearest mil)
2005	139	56,000,000
2006	346	50,000,000
2007	331	118,000,000
2008 [1 st half]	336	17,000,000
Total	971	239,000,000

 **SOCIETY OF CORPORATE
 COMPLIANCE AND ETHICS**  www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

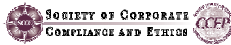
2

Data Losses are a global, industry-wide problem

Affected Industries:*



*2008 Data Breach Investigations Report by the Verizon Business Risk Team



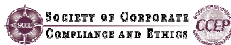
www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

3

Data Losses are a global, industry-wide problem

Interesting fact - no fact pattern:

- ✓ Gov/Schools/Military/Private business
- ✓ Large/medium/small companies
- ✓ Internal and external
- ✓ All modes of loss (hack/theft/lost shipment)
- ✓ Various storage media (laptop/thumbdrive/backup tape)
- ✓ Internet-based losses not a major factor but tend to get good publicity



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

4

Fifty Ways to lose your data...

✓ Lost laptops:

Some of the largest and medium-sized U.S. airports report close to **637,000** laptops lost each year, according to a Ponemon Institute survey. Laptops are most commonly lost at security checkpoints. Close to 10,278 laptops are reported lost every week at 36 of the largest U.S. airports, and 65% of them are not reclaimed.

✓ Lost thumbdrives

✓ Lost cellphones/Blackberries

✓ Theft of laptops from parked cars, on trains, planes etc

✓ Theft of computer equipment (including desktops and servers) from corporate facilities

✓ Hacks (external; employees)

✓ Corporate and state espionage

✓ Wireless interception (network; POS)

✓ Missing backup tapes/drives

✓ Lost or misrouted overnight packages



SOCIETY OF CORPORATE
COMPLIANCE AND ETHICS



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

5

Fifty Ways to lose your data...

✓ Emails sent to large group identified in “to” not “bcc” line

✓ Info sent inadvertently by email to unauthorized party

✓ Invoices sent to wrong customers (mail merge errors)

✓ Misrouted faxes

✓ Customer and/or employee information disclosed by phone to unauthorized party

✓ Inadvertant posting on the Internet

✓ Improper disposal

✓ Personal info disclosed in window of envelope in mass mailing

✓ Newspapers delivered in paper wrapping that includes SSNs or CC nos...



SOCIETY OF CORPORATE
COMPLIANCE AND ETHICS

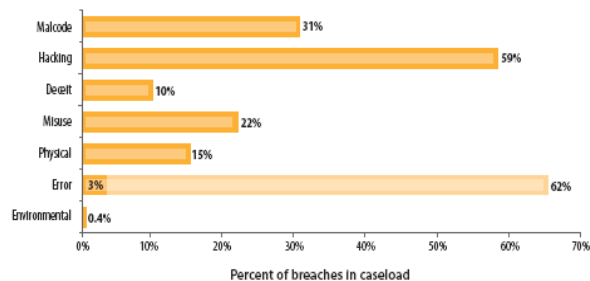


www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

6

It's real cybercrime, not just bored teens

- ✓ Data = \$\$\$
- ✓ The bad guys are selling the stolen data online and making LOTS of \$\$\$
- ✓ Increased use of sophisticated security threats to gather personal data: phishing; viruses; Trojan horses, keystroke loggers, rootkits etc.



* Chart from 2008 Data Breach Investigations Report by the Verizon Business Risk Team

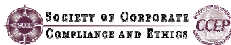


www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

7

Explosion of Breach Notification Laws

- ✓ Started in California
- ✓ Now 44 states in the U.S.,
 - Plus DC, Puerto Rico, Virgin Islands
- ✓ Imposes duty to disclose security breaches to –
 - Data subjects who may be affected/injured
 - Regulators/enforcement agencies (some laws)
 - Credit agencies (some laws)

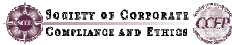


www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

8

Breach Notification Laws – Limited Scope

- ✓ Only require notice of a data breach
- ✓ There are other laws that:
 - create an obligation to keep data secure (5 states + several federal laws + the FTC)
 - govern use and display of SSNs (40 states)
 - govern data disposal (19 states)
 - create merchant liability in case of a data breach (1 state)
 - allow credit freeze (47 states)



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

9

Explosion of Breach Notification Laws

CSO Disclosure Series | Data Breach Notification Laws, State By State

Five years after California's landmark SB 1386, our interactive map shows you which 38 states have passed laws requiring companies to notify consumers whose personal information has been compromised. Part of an in-depth series about disclosing security breaches.

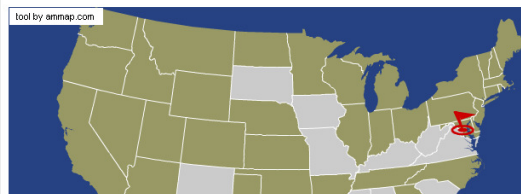
» Comments (3)

By Scott Berinato

February 12, 2008 — CSO —

More than five years after California's seminal data breach disclosure law, SB 1386, was enacted, not all states have followed suit. Eleven states still have not passed laws mandating that companies notify consumers when that company has lost the consumer's personal data. One state, Oklahoma, does have a breach notification law, but it only applies to state entities that have lost data.

That leaves 38 states that have enacted some sort of breach disclosure law. This map will help you sort them out. Click on any state to see highlights from that state's law. (The gray states do not yet have disclosure laws). For more explanation, see the text below the map. (To learn more, see the rest of the CSO Disclosure Series, including a deconstruction of two disclosure letters and an interview about pending federal legislation.)



tool by ammap.com

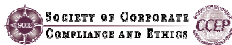
WATCH VIDEO TOUR

ESSENTIAL READING

- Network Security Basics
- Computer Incident Detection, Response, and Forensics
- Evaluating and Using Web Application Security Scanners
- The Future of AntiVirus
- The Complete Guide to Security Breach Disclosure

Don't miss out on the security content that your peers are receiving. **Subscribe to CSO Newsletters today!**

WEBCASTS



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

10

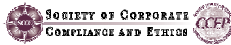
What Is Covered “Personal Data”?

Breach laws generally apply to certain combinations of personal data that can be used for ID theft

A person’s name Plus:

- ✓SSN
- ✓Drivers license number
- ✓Financial account or credit or debit card number:
 - “*in combination with any required security code, access code, or password that would permit access to financial account*” (30 states)
 - but only if circumstances exist wherein such number could be used without additional identifying information, access codes or passwords (3 states)
- ✓Other, e.g., Mother’s maiden name, DoB, medical information, biometric, etc. (in some states)

If data was encrypted – no need to notify (except Iowa), unless encryption key was lost with the data



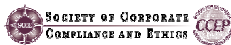
www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

11

What Is A Security Breach?

A security breach typically has two elements –

- ✓Unauthorized acquisition of computerized data,
- ✓That compromises the security, confidentiality, or integrity of personal information maintained by the business



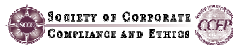
www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

12

When Does a Security Breach Trigger Notice?

The answer varies by state....

- ✓ Any breach of security, *or*
- ✓ Breach with some likelihood of harm
 - likelihood of loss or injury
 - likelihood of misuse of the information
 - risk of identity theft
- ✓ Harm standard varies
 - Not likely to
 - Not reasonably likely to
 - Not reasonably believed to
 - Not reasonably possible to
 - Will not cause
 - Does not create substantial risk of



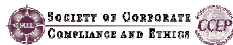
SOCIETY OF CORPORATE
COMPLIANCE AND ETHICS

www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

13

Key Differences in Breach Notification Laws

- ✓ Standard to trigger notice
- ✓ Affected Media : Computerized v. paper data (HI, IN, NC, SC, WI, MA)
- ✓ Residents vs. nonresidents (AZ, HI, NH, OR)
- ✓ Notification to state agencies or Credit Reporting Agency
 - NJ+MD require notice to law enforcement before customers notified
- ✓ Time to send the notice (10 days; 45 days; no delay etc)
- ✓ Method to send the notice and substitute notice rules (letter, email, web)
- ✓ Suspension of the time to send the notice at request of the authorities
- ✓ Requirements on what must be (or cannot be) communicated to affected individuals
- ✓ Private right of action (SC, AK)



SOCIETY OF CORPORATE
COMPLIANCE AND ETHICS

www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

14

Breach notification – not just the U.S.

- ✓ Japan
- ✓ European Union
 - European Commission recommends adoption
 - UK House of Lords Report recommends adoption
 - Norway
 - Some argue that already exists under EU law
- ✓ Canada - voluntary guidelines by IC
- ✓ New Zealand - voluntary guidelines by PC; seeking legislation
- ✓ Australia - same

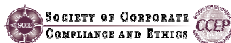


www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

15

Handling a Data Breach

- ❖ Not if – when...
- ❖ Breach impact:
 - ✓ Reputation/Brand
 - ✓ Market share/Shareholder value
 - ✓ Investors and potential investors
 - ✓ Customers/Consumers
 - ✓ Employees
 - ✓ Vendors/Third parties
 - ✓ Regulatory, legal and litigation



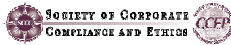
www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

16

Handling a Data Breach

Parties you may end up notifying:

- ✓ Law enforcement
- ✓ Credit bureaus
- ✓ Board of Directors
- ✓ Investors
- ✓ Regulatory agencies
- ✓ Privacy community
- ✓ Affected customers and/or businesses
- ✓ IT vendors/service providers
- ✓ Employees
- ✓ Media
- ✓ Your insurer

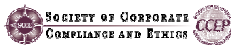


www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

17

The Incident Response Plan - why do I need one?

- ✓ Stay organized under pressure
- ✓ Make better decisions
- ✓ Minimize losses
- ✓ Mandated by regulatory agencies



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

18

The Incident Response Plan

1. Report incident to point person
2. Assemble Incident Response Team – Privacy, Legal, Compliance, IT, IS, HR, PR, Fraud or Loss Prevention, Audit, Insurance, Business Units, others?
3. Impact Assessment – nature and scope of breach
4. Containment:
 - ✓ Reduce potential impacted customers/Preserve company reputation
 - ✓ Restore integrity of all systems and data
 - ✓ Prevent further unauthorized access, disclosure
5. Internal Notifications
6. External Notifications
 - ✓ What to say
 - ✓ How to send
 - ✓ When to send
 - ✓ Who needs to be notified
 - ✓ Press release/media holding statement
7. Post Incident Management
 - ✓ Remediation
 - ✓ Control
 - ✓ Lessons learned



SOCIETY OF CORPORATE
COMPLIANCE AND ETHICS



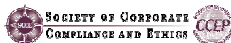
www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

19

The Incident Response Plan – more thoughts

Pre-incident:

- ✓ Be prepared – treat it like disaster recovery and have plans/resources ready and tested
- ✓ Have a structure but keep it loose – incidents tend to each be unique and raise their own issues and concerns
- ✓ Do NOT merely delegate this to the InfoSec team
- ✓ Do not assume your policies will protect you
- ✓ Do not assume encryption will protect you (but do encrypt as much as possible)
- ✓ Working with the police and other gov agencies – know the pros and cons and know in advance what your company's position is
- ✓ Be prepared to throw out all the rules and improvise... you will rarely have a textbook breach



SOCIETY OF CORPORATE
COMPLIANCE AND ETHICS



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

20

The Incident Response Plan – more thoughts

When an incident occurs:

- ✓ Project Management is critical
- ✓ Calculate your timelines – delay can cost you!!!
- ✓ Set up tasks and due dates
- ✓ Identify key personnel for each task
- ✓ Don't forget international aspects
- ✓ Don't forget this may end up in litigation – try to preserve your privilege
- ✓ Be prepared to throw out all the rules and improvise.....



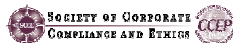
www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

21

Notifications - Content

Content should include:

- ✓ General description of incident
- ✓ Type of personal information compromised
- ✓ Steps company is taking to protect the information from further unauthorized access
- ✓ Further developments since the data of the breach
- ✓ Relief being offered by the company
- ✓ Advice on what the individual can do
 - Fraud alert recommendation
 - Review account activity recommendation
 - Other identity protection services
- ✓ Contact information in the event there are questions

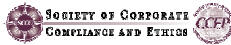


www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

22

Notifications - Other Considerations

- ✓ The mailings – internal or outsource?
 - Don't forget to sign NDAs if outsourcing this!
- ✓ Do all notifications have the same content?
 - Jurisdictional issues (MD = more; MA = less)
 - Employees vs. retirees vs. customers
- ✓ Less is better?
- ✓ Credit monitoring and other customer relief – negotiate in advance
- ✓ Further information –
 - Call Center or 800 number? – outsource or keep internal?
 - ❖ Train the call center team
 - ❖ Have escalation path for tough questions or belligerent callers
 - ❖ Assess international aspect (language, culture, timezone)
 - Whose name is on the letter
 - FAQs?

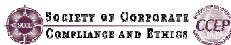


www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

23

Notifications - Other Considerations

- ✓ Who is the intended audience of the notification letters
 - The affected customers
 - Your employees (whether affected or not)
 - The regulators
 - The media
 - Others with a voice on the Internet
 - Plaintiffs' lawyers!!!



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

24

Some factors to consider in deciding if to notify

- ✓ What are the notification requirements where affected individuals live?
- ✓ How many people are in a breach notice jurisdiction vs those outside it
- ✓ What notification strategy has the organization followed in previous breaches?
- ✓ What countries are in play – what are local expectations?
- ✓ What are other companies in your industry doing?
- ✓ Are other companies part of the breach and what are they doing?
- ✓ Are you regulated?
- ✓ Are you exposed (high profile company? High profile breach? Multiple prior breaches?)

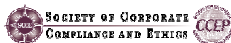


www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

25

Some factors to consider in deciding if to notify

- ✓ Potential Risks of Over-Notifying
 - Decline in stock value
 - Reputational loss
 - Loss of customers
 - “Notification Numbness”
 - Costs and administration of sending notifications and offering credit monitoring (for each breach incident)
 - Heightened regulatory scrutiny
 - Class actions



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

26

The press release or media holding statement

- ✓ Passive or proactive issuance of the press release
- ✓ FAQ?
- ✓ Do not conflict with what's in the customer notifications
- ✓ Legal should review and approve

Remediation steps

- ✓ “Hard” fixes - such as hard drive encryption
- ✓ “Policy” fixes - such as data access restrictions
- ✓ “Training” fixes - such as user awareness
- ✓ “Compliance/Enforcement” fixes - such as audits

Data Breaches and third parties

Contractual issues

- ✓ How soon should you get notice from the vendor
- ✓ Who sends the customer breach notification letters
- ✓ Who bears notification costs
- ✓ Notice in jurisdictions where not required
- ✓ Free credit reporting/monitoring/ID theft insurance
- ✓ Access to fraud resolution specialists
- ✓ Dedicated toll-free hotline
- ✓ Costs of investigations/lawsuits
- ✓ Cap on these costs???
- ✓ Increased cap in some circumstances?

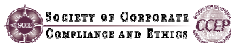


www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

29

Some potential breaches – no easy answers!

- ✓ Unauthorized Insider Access to Data
- ✓ Unauthorized Outsider Access to Data
 - What if they are subject to an obligation of confidentiality?
- ✓ Lost device that is recovered and there is forensic proof the data wasn't accessed
- ✓ Lost backup tape – definitely somewhere in your offsite storage facility but no-one can find it...
- ✓ Lost backup tape – data inaccessible (but unencrypted)
- ✓ Lost laptop and no-one knows what was on it
- ✓ Hack to a system with lots of data and no trail of what if any data was accessed or stolen



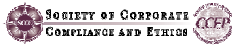
www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

30

Questions?

orrie.dinstein@ge.com

(646) 428-7129



www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977