What Happens After the Lights Go Out?

By John C. Checco, CISSP, CSSLP

2008 was not a good year by any standard. As many of us try to rebuild our careers, our finances and some semblance of normality,; data privacy and information security is probably farthest from any company's (or any individual's) objectives for 2009. And that's when information theft becomes most opportunistic.

As companies fold, merge or experience massive reorganizations, there emerges an excess of unsupervised personally identifiable information (PII) – whether it be through former employees, surplus equipment or forgotten databases. Although every company has a legal obligation to destroy any sensitive data as part of their exit strategy, by the time an information leak has been discovered there may no contact information for the defunct company.

Consider the following distinct cases:

1) It was reported in January of 2009 that patients' records for [now-defunct] Houston "Express EMS Services" was found in a parking lot and dumpster.[1]

2) Former employees of [now-defunct] L.G. Defelice Inc. had their Social Security Numbers posted on the web from improperly sanitized data retrieved from the DOT about the former company.[2]

3) The former NY United Hospital offered to make its records available to patients for six months while it was executing its closing procedure. As part of its exit process, the hospital prepaid a third party to store any remaining records for a period of seven years; upon which they will be destroyed.[3] The records are retrievable, but the only requirement for authorization is a signature; the verification of which is impractical.

4) Client records from a mortgage broker "Seaview Financial of Corona del Mar" were found in a recycling bin during the company relocation in February of 2009.[4]

---

[1] References:
- http://datalossdb.org/incidents/1495-medical-records-of-defunct-ambulance-company-s-patients-found-in-parking-lot-and-dumpster
- http://abclocal.go.com/ktrk/story?section=news/local&id=6605230

[2] References:
- http://datalossdb.org/incidents/734-social-security-numbers-of-300-former-employees-of-defunct-l-g-defelice-inc-posted-on-ct-transportation-committee-website
- http://attrition.org/dataloss/2007/07/conngatc01.html

[3] References:
- http://www.allbusiness.com/health-care/health-care-facilities-nursing/10635002-1.html
- http://www.ironmountain.com/records/release/NYunited.asp
- Interview with Iron Mountain records release specialist for NY United Hospital

[4] References:
- http://datalossdb.org/incidents/1791-mortgage-broker-dumps-files-containing-clients-names-address-tax-forms-and-ssn-in-trash
- http://www.ocregister.com/articles/information-seaview-files-2316272-center-recycling

5) A large consumer electronics firm, upon exercising its exit strategy, considered two alternatives for data disposal: electronic wiping or physical destruction of storage. (It was found more cost effective to physically destroy the disk drives.)[5]

And the list goes on and on… perusing "DataLossDB.org" will give one nightmares on the inefficacy of data protection in the real world. The fact that the volume of incidents is large enough to be aggregated by industry, breach type, and information type is a disturbing indication on how extensive the problem of information leakage is.

The Perfect Storm

This economy has created a "perfect storm" for identity fraud to thrive and grow.

Given three straight fiscal quarters of economic downsizing, the probability increases that companies which succumbed to the economic crisis will inadvertently fail to properly dispose of their sensitive data.

As the unemployment rate reaches record proportions, the propensity of identity misuse – even something as simple as parents using their children's SSN to get more credit – increases as well. (A study in 2008 found approximately 5% of families surveyed had children with compromised identity information[6].)

From a market perspective, higher unemployment means the *quality* of current identity data decreases, poisoning the supply chain. As a consequence, the price of PII drops dramatically, so *quantity* needs to increase to maintain the present market levels.

Law and Responsibility

There are many regulations and guidelines specifying the protection and proper destruction of sensitive information.

 HIPAA has long been criticized for its overly broad requirements prone to ambiguous and sometimes contradictory interpretation. Yet, this is one of the few regulations that mandates organizations to make accommodations for the proper storage and disposal of information for six years, even after an organization's operations ceases[7].

 There are several New York State laws that require businesses to follow a data retention schedule for information[8]. Although these retention and disposal requirements are subject to legal interpretation, conservative legal council should follow the path of least risk and provision for post-operational protection.

[5] Interview with CTO [person's name removed by request] from [company name removed by request].
[6] Reference: http://www.debix.com/docs/Child_ID_Theft_Study_2008.10.pdf
[7] Reference: http://www.glrm-online.com/pdfs/HIPAA Record Retention Periods 2006.pdf
[8] Reference: http://www.archives.nysed.gov/a/records/mr_retention.shtml

- The Fair and Accurate Credit Transaction Act of 2003 (FACTA) Disposal Rule "requires disposal practices that are reasonable and appropriate to prevent the unauthorized access to – or use of – information in a consumer report"[9], but it fails to explicitly specify if "reasonable" includes contingency plans if the responsible party ceases operations.

- The Gramm-Leach-Bliley Act Safeguards Rule is also quite specific about information protection with U.S.C. Title 15, Chapter 94, "Subchapter I: DISCLOSURE OF NONPUBLIC PERSONAL INFORMATION" and "Subchapter II: FRAUDULENT ACCESS TO FINANCIAL INFORMATION "[10]. There are specific rules for safeguarding nonpublic personal information as well as the communication of privacy protection practices. Yet, even in GLBA there is an interpretation loophole. Although the protection of PII extends to "information of those no longer consumers of the financial institution,[11]" it is unclear if it the responsibility applies if the "broken relationship" is caused by the company's demise.

- The reference to "internal controls" of Sarbanes-Oxley section 302 cannot be interpreted purely in the accounting sense; it pertains to information leakage if the lack of (or management overriding of) controls can lead to fraudulent activity or non-compliance. In Seaview Financial's case above, there is a clear violation; but what about the similar situation with Express EMS Services? Do internal controls cease to be in effect if the company is no longer operating?

Some legal experts believe more specific regulations are detrimental and that bankruptcy courts should address the interpretation of existing regulations with regard to data protection extensions.[12]

The Sedona Conference – a consortium of legal experts – has created "Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age"[13]. This guideline is followed by many legal professionals; and provides an ideal platform to specifically address these post-mortem data protection issues from a legal perspective.

The Reality

Most of the executives interviewed were not aware of any regulatory requirements for post-operational retention/disposal of data in their industries; although some were aware that their companies do have such plans and others have even exercised such plans with former employers.

Looking into the problem more deeply, the root cause comes down to human error in three distinct ways:

1) Lack of awareness or identification of sensitive information by employers, employees, vendors, clients and end users.
2) Explicit negligence to follow proper information protection and disposal procedures; where operational efficiency outweighs privacy rules and regulations.

[9] Reference: http://www.ftc.gov/opa/2005/06/disposal.shtm
[10] Reference: http://www.law.cornell.edu/uscode/uscode15/usc_sup_01_15_10_94.html
[11] Reference: http://en.wikipedia.org/wiki/Gramm-Leach-Bliley_Act#Safeguards_Rule
[12] Reference: Interview with legal experts [names withheld by request].
[13] Reference: http://www.thesedonaconference.org/dltForm?did=Guidelines.pdf

3) Failure of technology to classify and protect electronic information by both technology developers as well as users.

We need to be aware of how information affects each and every one of us:

> As keepers of the information: The information protection priority for every CIO (or CPO) should always be effectiveness before efficiency.
>
> As users of the information: Every employee has an obligation to protect client information as well as ensuring their own PII is well protected and supervised.
>
> As owners of the information: As vested clients of various financial, medical and other institutions, we need to reach out and request the formal policies for data retention and destruction. As with the case of United Hospital above, there was a court-approved plan in place for proper handling and disposal of client data.

The National Association for Information Destruction (NAID) provides a checklist for ensuring your company complies with the maximum set of regulatory requirements[14].

In Summary

Although very few regulations explicitly address post-operational conditions, there is an interpretative factor with any regulation that defines specific schedules for data retention and disposal:

Are records retention/disposal requirements in effect beyond the life of the organization?

There is no clear answer to this question. For records that transcend a company's purpose – medical record being the most obvious example – there needs to be better data retention policies. Conversely, for consumer data that is only relevant to the operations of a company, common sense dictates the disposal of this information at the proper time.

Hence, we need a robust Information Lifecycle Management (ILM) initiative.

Information privacy, protection and governance are more difficult, more expensive and more costly in times of instability. Considering the frequency of information leaks in active companies; the exposure of PII gets exponentially greater once a company ceases operations. It is imperative that your enterprise's protection plans outlive the company.

About the Author

John C. Checco, CISSP, CSSLP, is an information security consultant. He may be reached at Checco Services, 845-942-4246 or via email at john.checco@checco.com.

[14] Reference: http://www.naidonline.org/facts.html