Estimating the Costs of a Data Breach: An Exercise at the New Hampshire State Cancer Registry

Bruce Riddle[1], Steve Nyman[2], Judy Rees[1]

[1]New Hampshire State Cancer Registry, [2]Chief Information Security Officer, Dartmouth College

Background

Following a risk assessment undertaken at Dartmouth College, NHSCR performed a planning exercise to estimate what a data breach might cost our supporting institution.

In information security, risk is defined as "the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization." [1] Exposure is an estimate of the potential losses. If you leave a $20 bill on the sidewalk, the risk is high that it will be stolen but the exposure is low. The potential risk for a central cancer registry is unauthorized access to personal and medical records due to theft, loss or electronic access to a data server or field laptop; and loss of documents from the office.

Many states require notification of breaches to a central registry [eg 2] which lists all breaches and makes documentation of the response available for public scrutiny. In 2009, a breach was discovered at the Carolina Mammography Registry, affecting up to 180,000 patients [3]. Each patient was sent a long explanatory document with detailed information about the breach. The financial costs of that particular breach are unclear, but the intangible costs at other mammography registries and elsewhere were extensive.

Table 1: Potential costs associated with a central registry data breach

Intangible Costs	Tangible Costs
• Breach of trust between citizens and institution • Inconvenience for citizens (risk of identity theft and counter-measures) • Damage to the reputation of the institution as a data custodian and steward of public health information • Damage to other activities at institution, (eg registries, research studies, clinical trials) • Adverse publicity for public health and national agencies, (eg NPCR, NAACCR, SEER) • Reduced political support for registries with potential budgetary consequences	• Costs of IT staff to evaluate and contain breach and initiate breach response • Certified letters to all persons or person's families in registry • Credit monitoring of all living persons • Legal fees to attorneys supervising breach follow-up and defending institution • Civil and criminal fines • Fees for external auditors • Costs of public relations efforts • Termination of business contract

The Ponemon Institute, sponsored this year by the computer security company, Symantec, publishes an annual report on the cost of a data breach [4]. The most recent survey estimates the total cost of data breaches in a commercial setting as follows:

Table 2. Estimated total costs of data breaches

	Cost per breached record
Overall mean total costs	**$214**
Institutions with a first data breach, total costs	**$326**
Institutions who responded quickly (<30 days), total costs	**$268**
Institutions who responded slowly (>30 days), total costs	**$174**
Direct costs only	**$73**

Of note, institutions face higher costs the first time a breach happens. Another interesting finding was the increased cost among faster responders, which was attributed to early, unnecessary notification of individuals whose records were thought to have been breached. Subsequent information showed that notification in many cases had been unnecessary.

Some of the costs in Ponemon's model do not apply directly to the registry world, such as loss of existing or future customers. Economies of scale also need to be considered when interpreting these data.

Analyses

New Hampshire has a population of 1.2 million with approximately 7000 new cancers diagnosed annually [5]. Data have been collected since 1987. The following exercises assume loss of unencrypted personal health data. The mitigating effects of encryption and other security measures that we use in NH are discussed later.

Exercise 1: Direct Costs

Assumptions:

Unique individuals' records in the database	155,693
Individuals presumed to be alive	104,391 (67%)
Direct costs of a breach, per individual [4]	$73

Using Ponemon's data, the estimated direct costs of a breach are $73 per compromised record. This gives estimated directs costs of a breach as follows:

155,693 x $73 =	$11,365,589	if all patients are included in the response
104,391 living x $73 =	$7,620,543	if only living patients are included

Exercise 2: Fines

Like many cancer registries we collect cases on out of state residents, which in New Hampshire comprise about 14% of unique individuals in our database. A few states have implemented computer breach and notification laws that may come into play in the event of a breach. For example, Massachusetts can impose fines of $5000 per case [6,7].

Assumptions:

MA records in our database	1,605 (1.0%)
Fine per breached record	$5,000

Under these assumptions, a breach might cost New Hampshire $8,025,000 in fines for Massachusetts alone, which would be added to the costs estimated in Exercise 1 for a total of over $15.6 million.

Exercise 3: Risk Modeling

Data breach liability calculators developed by interested parties are available on the internet, for example, by Symantec in conjunction with the Ponemon Institute [8], and Tech//404 [9]. Again using 155,693 unique persons, the latter calculator gives some rough estimates of potential loss. A subtotal removes regulatory investigation defense and state/federal fines or fees.

We note the potential for over-estimation by modeling software products developed by computer security or liability insurance companies, as well as difficulties applying models developed for the commercial setting in a public health setting. These factors should be considered in the interpretation.

Table 3. Tech//404 cost estimator for a data breach [9]

		-20%	Average Cost	20%
A.	**Internal Investigation***			
1	Cybercrime consulting	$420,274	$525,343	$630,411
2	Attorney fees	$426,121	$532,652	$639,182
		$846,396	$1,057,995	$1,269,594
B.	**Notification/crisis management***			
1	Customer notification, certified mail	$774,766	$968,458	$1,162,150
2	Call center support	$548,184	$685,230	$822,276
3	Crisis management consulting	$306,983	$383,729	$460,474
4	Media management	$60,666	$75,832	$90,998
		$1,690,599	$2,113,248	$2,535,898
C.	**Regulatory/compliance**			
1	Credit monitoring for customers*	$3,522,994	$4,403,743	$5,284,491
2	Regulatory investigation defense	$1,303,215	$1,629,019	$1,954,923
3	State/federal fines or fees	$2,764,308	$3,455,385	$4,146,462
		$7,590,518	$9,488,147	$11,385,877
Total data loss expenses		**$10,127,512**	**$12,659,390**	**$15,191,368**
Selected Subset Applicable to Registry *		**$6,059,989**	**$7,574,986**	**$9,089,983**

Note: Totals may not add up due to rounding

Discussion

If commercial models can be applied to the registry setting, direct costs of over $7 million might result from a data breach with loss of unencrypted personal health data at a small central registry. Larger registries that have been operating for longer would have substantially larger potential exposures. These estimates should be interpreted with caution as they were based on commercial modeling and do not allow for economies of scale in estimating costs of a response protocol.

In practice, the true cost of a breach will be lower if better security measures are in place. Put another way, improvements in security may change the definition of a true breach. For example, loss of an encrypted laptop with two-factor authentication, such as those used in New Hampshire, would pose a very small risk of access to personal data, and notification of individuals may not be necessary. In contrast, unencrypted data on a lost laptop protected by a simple password is essentially unprotected. Tangible and intangible costs could be massively reduced if only encrypted, inaccessible data were lost.

We believe, given all the procedures and practices we have implemented and our ongoing scrutiny to optimize security, our potential risk is relatively low. We are discussing ways to optimize data security in New Hampshire even further.

A data breach at any cancer registry carries a large potential exposure for intangible costs both locally and nationally and would have serious repercussion for other registry and public health activities across the country.

References

1. 1ISO/IEC 27005:2008 http://www.iso.org/iso/catalogue_detail?csnumber=42107
2. http://doj.nh.gov/consumer/breaches.html
3. http://www.unc.edu/cmr/breach.shtml
4. 2010 Annual Study: U.S. Cost of a Data Breach, March 2011, Symantec Corporation
5. Personal communication, Sai Cherala, MD, NH Department of Public Health Services
6. http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf
7. http://www.malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93A/Section4
8. https://databreachcalculator.com/
9. http://www.tech-404.com/

This project was supported in part by the Centers for Disease Control and Prevention's National Program of Cancer Registries, cooperative agreement U58/DP000798 awarded to the New Hampshire Department of Health and Human Services, Division of Public Health Services, Bureau of Public Health Statistics and Informatics, Office of Health Statistics and Data Management. Its contents are solely the responsibility of the authors and do not necessarily represent the official views of the Centers for Disease Control and Prevention or New Hampshire Department of Health and Human Services.