CLEARWATER COMPLIANCE
Healthcare Cyber Risk Management Solutions

**Determining the True Cost of a Data Breach**

By Barry Mathis, Senior Vice President and Chief Business Development Officer, Clearwater Compliance

Health care organizations are under attack. So much so, that it is no longer a matter of "if" your organization will suffer a data breach, but "when." According to a report from the Ponemon Institute, nearly 9 of 10 health care organizations experienced at least one data breach within the past two years. And nearly half experienced more than five breaches in the same time period.[1]

In response, health care organizations are investing resources in information risk management (IRM), including appointment of chief information security officers (CISOs), investing in technology talent, training employees in cyber awareness, and implementing new technology. But with multiple competing budget priorities, organizations struggle to identify the right amount of resources to allocate to IRM.

After all, investing in IRM is not as simple as decisions to invest in new lines of business. In new business decisions, estimating return on investment can be fairly straightforward. But when a health care organization is investing in IRM, the question becomes less about "What do we have to gain?" through investment, and more about "What do we stand to lose?" if such investment isn't made.

That's why it's important to understand the true cost of a data breach. Understanding the total potential financial impact helps provide context for discussions about allocating resources to IRM.

**Calculating the Cost of a Breach**

Many methods are available for calculating the cost of a breach. One quick way is to use the Ponemon Institute's cost-per-compromised-record figure to come up with an estimate. The most recent Ponemon study estimates the cost per compromised record for the health care industry at $380 (global figure).[2] That is, a data breach involving 10,000 records is projected to cost roughly 10,000 x $380, for a total of 3.8 million dollars. But this is only a starting point.

An alternative method for calculating costs is to use the Protected Health Information value estimator (PHIve) developed by the American National Standards Institute.[3] Using the five-step PHIve method, organizations conduct a risk assessment; determine a security readiness score; assess the relevance of cost; determine impact; and then calculate the total cost of a breach. Individual, accurate estimates cannot be developed without progressing through all five steps.

---

[1] Ponemon Institute. *Sixth Annual Benchmark Study on Privacy & Security of Health care Data*. May 2016. Retrieved from www.ponemon.org

[2] Ponemon Institute. *2017 Cost of Data Breach Study: Global Overview*. June 2017. Retrieved from https://www.ibm.com/security/data-breach

[3] *See* ANSI. *The Financial Impact of Breached Protected Health Information: A Business Case for Enhanced PHI Security*. 2012. Retrieved from https://clearwatercompliance.com/wp-content/uploads/2014/07/1-6.-The-Financial-Impact-of-Breached-Protected-Health-Information.pdf and The PHI Protection Network. *The Financial Impact of Breached Protected Health Information: 2017 Update*. Retrieved from http://www.phiprotectors.org/2017-white-paper-update

Clearwater Compliance has developed a PHIve-based model for estimating the true cost of a data breach. Clearwater's model incorporates an organization's total annual revenues, an estimate for the number of records breached and five broad categories of repercussions to develop a total cost estimate. The five categories of repercussions include:

**REPUTATION**

An organization's good reputation is a valuable asset. A positive brand builds trust and loyalty between the organization and its patients, potential patients, clinicians, workforce and strategic partners. The fallout from a data breach can damage this trust, and organizations may lose current revenues due to a higher than normal loss of customers (i.e., abnormal churn rate) as a result.

One study found the abnormal churn rate in the health care sector after a data breach was 6.7 percent.[4] Multiply 6.7 percent by your total annual revenues to get an idea of the revenue loss you might incur due to this single factor.

Of course, reputational damage has other repercussions as well. Negative publicity related to a data breach may dissuade new customers from choosing your organization in the future, leading to a loss of new revenues. Staff may resign, requiring your organization to invest in recruitment and training of new personnel. Strategic partners may also reconsider their relationship with your organization after a data breach.

**FINANCES**

Financial repercussions include the costs of remediation, mitigation and notification. Remediation refers specifically to the costs associated with limiting further use or disclosure. These might include the costs of conducting a forensic investigation, assessment or audit, and implementing crisis management. Providing credit and identity theft monitoring for impacted individuals is often a part of remediation as well.

Mitigation refers to the costs associated with ensuring that a similar breach doesn't happen again. Depending upon the situation, mitigation might include encrypting all laptops, replacing lost or stolen assets and retraining the workforce.

HIPAA has specific requirements for notification of impacted individuals and the media in the case of a data breach.[5] Costs associated with notification might include a per-record cost for notifications to impacted individuals, as well as costs associated with providing call center support. A call center is frequently set up after a breach to field calls, answer questions, and provide information about enrolling in credit monitoring or ID theft management programs. Media notification costs may include securing crisis management counseling and/or media management services, as well as attorney's fees. These costs will likely scale with the number of records impacted by the breach.

---

[4] Ponemon Institute. *2016 Cost of Data Breach Study: United States*. June 2016.
[5] 45 CFR § 164

Additional financial repercussions include the cost of cyber liability insurance. Some insurers have instituted limits on the cyber liability policies they issue to an organization that has experienced a significant data breach. If your organization has cyber liability insurance in place, you will want to consider the cost of the deductible, as well as the cost of any premium increase, when a data breach occurs.

**LEGAL AND REGULATORY REPERCUSSIONS**

The direct costs associated with the legal and regulatory repercussions of a data breach are often the first costs that come to mind. These include fines and penalties imposed by the U.S. Department of Health and Human Services, Office for Civil Rights (OCR). Settlements with OCR can easily reach into the millions of dollars. The size of the breach and the culpability of the organization directly impact the fees and penalties imposed. One of the larger settlements ever imposed against a single entity was a $5.55 million settlement OCR imposed on Advocate Health Care in 2016.[6]

OCR can also impose Corrective Action Plans (CAPs) on organizations they find to be out of compliance with HIPAA. CAPs specify actions organizations must take to comply with HIPAA. CAPs may entail developing and documenting new policies and procedures; developing and implementing workforce training; implementing new safeguards; conducting a risk analysis; and hiring an independent monitor to evaluate and report on the organization's progress. The costs of CAP compliance can be extensive.

In addition to the costs associated with OCR actions, many states (including Arkansas), have their own laws regarding data breaches. Finally, don't forget the potential for a class-action lawsuit.

**OPERATIONAL REPERCUSSIONS**

Operational repercussions might include hiring and training additional staff to support improved security and privacy beyond the measures specified in a CAP. In addition, staff churn in the wake of a data breach may necessitate reorganization. An example might be moving the CISO or security officer under general counsel, or under the Board, rather than reporting to the Chief Information Officer.

**CLINICAL REPERCUSSIONS**

Potential clinical repercussions, though hard to quantify, should also be included in any calculation of data breach costs. Has the data breach led to the submission of fraudulent claims? Has the integrity of patient records been compromised? Have patients suffered harm due to compromised data? Has the data supporting clinical research or clinical trials been contaminated? Any one of these situations has associated liabilities which must be considered when calculating total cost.

---

[6] Office of Civil Rights Press Office. *Advocate Health Care Settles Potential HIPAA Penalties for $5.55 Million*. Aug. 4, 2016. Retrieved from http://wayback.archive-it.org/3926/20170129041109/https://www.hhs.gov/about/news/2016/08/04/advocate-health-care-settles-potential-hipaa-penalties-555-million.html

**THE BOTTOM LINE**

It should be clear that a data breach initiates a multitude of consequences. Some consequences have direct and obvious costs; some have costs that are harder to quantify but are still relevant. When you consider the impacts of all possible repercussions, the total cost of a data breach may well exceed the average per record cost published by the Ponemon Institute.

An organization's ability to build a persuasive business case for increased investment in IRM is dependent upon its ability to articulate the true cost of a data breach. At the same time, it's important to remember that health care organizations have much to gain from their investments in IRM.

A robust IRM program can lead to stronger financials by mitigating losses due to data breaches. A robust IRM program can contribute to more competitive insurance rates. A robust IRM program can contribute to higher satisfaction among patients, physicians, workforce members, the Board, investors and the community. And most importantly, a robust IRM program protects patients by ensuring access to quality care, facilitated by the security of their protected health information. That is the true return on investment for an organization's investment in information risk management.