

Cyber Strategy and Enterprise Risk Management (ERM)

By Albert L. Sica and Jonathan Edwards

October, 2015

I just returned back from an excellent ERM workshop hosted by NC State University. The workshop highlighted many issues directly impacting the maturity of ERM within companies. These issues coupled with a few excellent articles in the October issue of RIMS magazine ([Developing a Cyberbreach Strategy](#), [Helping the C-Suite Assess Cyberrisk](#)) sets the stage for how Cyber Risk and ERM might be a great marriage for any company.

The principles surrounding ERM are positioned to help a company identify, qualify, quantify and determine mitigation strategies to thwart its exposure to different risks such as a data breach. The concept of [Risk Appetite and Risk Tolerance](#) are important concepts when thinking about the magnitude of the financial impact of a data breach. With the expenses tied to a breach rapidly escalating it doesn't take long for an organization to incur astronomical and potentially "show stopping" costs.

Expenses for a data breach typically include items such as regulatory fines and penalties, notification expenses, crisis management expenses, and legal fees and legislation surrounding the reporting of a data breach only exacerbates the potential costs and litigation. This summary from Baker Law provides a very nice overview of the state-by-state guidelines. Click to read the [BakerHostetler Data Breach Charts](#).

The latest [Ponemon/IBM Study](#) on the cost of a data breach indicates it would approach \$217/record so with, say, 1,000,000 records which may be compromised you can see the magnitude of the problem. While this is a "scary" number and

one which could bankrupt many companies, there is simply not enough commercially available insurance to cover these [direct] costs not to mention things like Reputational Risk or consequential losses the organization could endure from additional security or engineering costs. The commercial insurance market will challenge organizations with areas such as 1) cost of coverage; 2) retentions/deductibles imposed; 3) potential sub-limits of coverage for critical areas; and, 4) the organization's ability to cover acts that happened prior to the inception of the coverage ("prior acts").

For precisely this reason companies need to take a broader, more methodical approach to identifying risk exposures and areas within the organization that could precipitate an event. Applying basic ERM framework steps to ring-fence loss potential and clearly identifying demonstrable and auditable steps that the business has taken to mitigate the exposure will allow senior management to have greater clarity of the volatility of the risk exposures.

Enterprise Risk Management is there to reduce surprises, increase certainty and document steps taken to mitigate exposures. A very remedial view

Albert Sica is the founder and Managing Principal of The ALS Group. For more information, call 732.395.4251 or e-mail Al at asica@thealsgroup.com.

Jonathan Edwards, is an IT and cyber-risk specialist at The ALS Group. For more information, call Jon at 732.395.4281 or e-mail him at jedwards@thealsgroup.com.

is "What can go wrong? How bad can it get? What can I do about it? Is that solution sustainable?" That is the "DNA" of risk management. An often overlooked benefit from proper risk management is that greater awareness which allows the organization to exploit opportunities they may not otherwise be comfortable undertaking. A great example of this is the Chinese symbol of Risk which allows for both positive and negative outcomes and is a combination of danger (crisis) and opportunity representing the downside and upside of risk.¹


危險

Enterprise Risk Management does not have to be overly complex or cumbersome. In fact, that is why many companies start out with the concept but never mature it fully within the organization.

Here are a couple of key elements that we would suggest be considered and adopted when designing a risk framework:

- **Establish a Risk Management Committee** – a cross-functional group of company leadership that is charged by an executive committee member to create and administrate the ERM process. That group should have a Charter that is simple but yet expresses the company's desire to conduct thoughtful risk reviews.
- **Determine Risk Appetite and Risk Tolerance** – this is a very elusive concept to many but should form the basis of your materiality chart. Risk Appetite and Risk Tolerance should be expressed numerically and with a full understanding of financial statements, stakeholder expectations, lending covenants etc.

¹ <http://people.stern.nyu.edu/adamodar/pdfiles/valrisk/ch1.pdf>

- **Establish Risk Materiality** - this is a scale that is tied to the numeric results in your Risk Appetite and Tolerance figures. Risk is a product of frequency and severity. These measures should be tied to a recognized standard (ISO 31000, COSO, etc.). We like to use a simple Red/Amber/Green scale 
- **Establish Risk Categories** - the categories can be established that will allow the organization to start to think about risks in "buckets". It would be natural to then think about an "owner" of that "bucket" of risks which feeds into the organizations risk work-group.
- **Have a Common Language** – whatever "standard" the company chooses use terminology that is aligned with that standard. All the recognized global standards have a definitions section that allows for that "common language"
- **Create a Risk Register** – this is one of the areas that begins the complexity and cumbersome tendency. Think of your risk register as the accountants work-papers. No senior executive reviews work-paper minutia and they should not start now. Each Sr. Leader of the Risk Committee should have their delegates that use the established framework above to identify all the risks they can think of and then rate them. Any above a certain threshold should then be considered by the committee. This is precisely why the Risk Materiality is so important – it keeps senior leadership out of the "weeds". There are many versions of what a proper risk register should look like – try to keep it as simple as possible while still allowing anyone to understand the risk,

category, owner, frequency, severity and what management controls are in place to mitigate that risk.

- Now that you have a risk framework in place you can use that framework to examine areas that would give rise to a data breach and, potentially, have catastrophic results. Your considerations can include the areas of concern, what type of Private Data² is handled in the company and how it may be exposed. A critical area to consider is a Public Relations – Breach Notification Plan – a simple “how to” guide on what should be done in case of a data breach.
- Data breaches happen both within the companies themselves and with vendors that a company may engage to perform services. The Target data breach, for example, started with a vendor of Target that allowed for a pathway to the intrusion. Because of situations such as this, it is important that the ERM process considers ALL sources of risk both within the company and with outside vendors.
- While the topic of Cyber Security is a top risk on the minds of most senior leadership, it is not always apparent the company has a methodical way to consider and manage the risks that can manifest into an exposure. Adopting an Enterprise Risk Management framework is an ideal way to

allow the company to have a defined process to work through these exposures.

About The ALS Group

The ALS Group is an independent insurance and risk management advisory firm located in Edison, N.J. The company was founded in 1993 and serves as an advocate for its clients, and since it does not broker or sell insurance or accept engagements from insurance carriers or brokers, its perspective is uncompromised. The ALS Group is one of the largest independent risk management advisory firms in the United States, offering services to business & industry both nationally and internationally.

For more information:

- www.thealsgroup.com
- info@thealsgroup.com
- (732) 395-4250.

² As defined in State Technology Law, shall mean personal information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted or encrypted with an encryption key that has also been acquired:

- social security number;
- driver's license number or non-driver identification card number; or
- account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account. Private information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.