cytegic

CYBER SECURITY
MANAGEMENT SOLUTIONS

White Paper

A method for estimating the potential financial impact of cybercrime

Version 1.0

March 2016

Abstract

Cytegic has developed an integrated platform for risk managers and information security officers. Cytegic helps translate the security posture of an organization into a risk profile inclusive of the financial cushion required to cover expected losses from cybercrime. Computation is based on the aggregation of reference information from the market and the internal prioritization of assets and risks. Deployment is rapid and simple with the use of the embedded wizard, however fine-tuning is highly recommended to best represent the risk profile of the organization.

The Process

1. External data gathering

Defining the baseline for financial impact requires two numbers - estimated financial impact of **severe** attacks during relevant period (usually one year) and the estimated financial impact of **mild** attacks during that period of time. The underlying assumption is that no organization is expected to have a full year free of cyber attacks however, the severity of these attacks may range from minimal financial impact to extremely severe. The actual risk number will be referenced to these encore points.

Sources of such estimation are: published reports such as Ponemon, benchmarking with comparable organizations, industry-related insurance publications, case studies and yearly reports from consulting firms. The current legislation requesting enterprises to report all cyber attacks and their financial impact makes this estimation much more reliable. However, one may not expect these numbers will be relevant to a specific organization “out of the box”. Even if you find published numbers relevant to your specific organization, expert analysis should be executed to represent differences in geo-political locations, business style, group companies that may reflect on the risk profile, events and changes in threat landscape.

Since the process of updating estimates is very simple, a simulation approach is recommended utilizing a variety of scenarios computing the financial outcome under several assumptions.

2. Setting priorities

Priorities should be set, per business environment, for two factors: asset priority and objective priority.

Asset priority relates to the list of assets residing in the relevant business environment. Assets, such as business transactions, clients’ data, intellectual property and others, may be relevant to a specific business environment to a greater or lesser importance. For example, engineering division may prioritize IP as top priority while sales will relate to client’s data as crown jewels.

These priorities are translated internally into the computation coefficients for

each asset. Priority of assets is not a must and the system will work just fine with equal importance to all assets.

Objectives are the motivations of the attacker to execute manipulation on data and systems. The current standard relates to confidentiality, integrity and availability.

Confidentiality related to exposing secret information to unauthorized parties, Integrity relates to data manipulation such as changing the routing number of financial transaction, Accessibility relates to disruption of service or blocking access to operations such as ransomware.

Allocation of value to each objective represents expected severity of each objective on the business operations. In some cases, data leakage may be the key risk for a business while in other cases accessibility to processes is a must. Since the cyber impact may be a result of each objective the default value is 100% for each objective and updating it according to organization profile will make computations that much more specific and accurate.

3. Cyber financial resilience Wizard

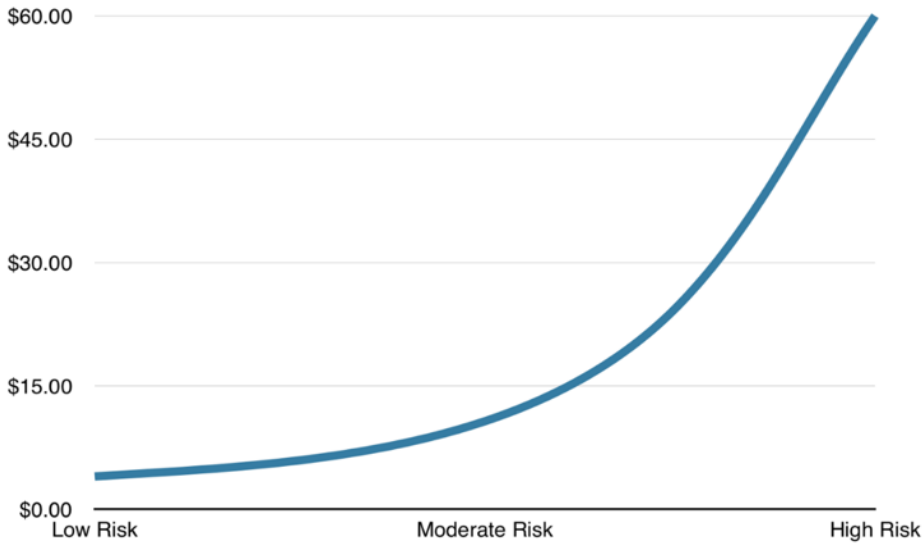
The objective of the wizard is to provide main-effect extrapolation of the external inputs and internal priorities into specific financial impact range per asset per objective. Using only a few data points the wizard breaks-down the risk expectancy for each asset per each objective and populates the financial database to be the reference for the specific financial impact per current security posture. The internal process of the wizard is two staged - first stage computes the specific percentage allocation allocation per each objective X asset combination. Second stage allocates the financial reference numbers in proportion to the percentage distribution.

4. Fine tuning

The fully populated financial database may, and should, be fine-tuned post wizard operations. While the wizard computes all main effects into asset X objective cells some specific adjustments may be required. For example, it could be that although the highest priority is to data leakage the relevance of that objective to business process could be marginal however accessibility is a must. A review of the outcomes of the wizard computation per specific cells may increase the accuracy of data representation while the bulk of cells may remain populated by the wizard.

5. Risk and impact computation

Computation of financial impact is an integral part of the assessment calculation in the system. Regardless if the computation is done automatically during revolving presentation mode or specifically per update the system computes all risk scores per assets and environments. The financial impact is extrapolated from the current risk score per each asset per each objective. The financial impact correlation with the risk score is curvilinear since increase of risk from 4 to 5 (5 being to of the scale) has a much higher impact than increase of risk score from 1 to 2.

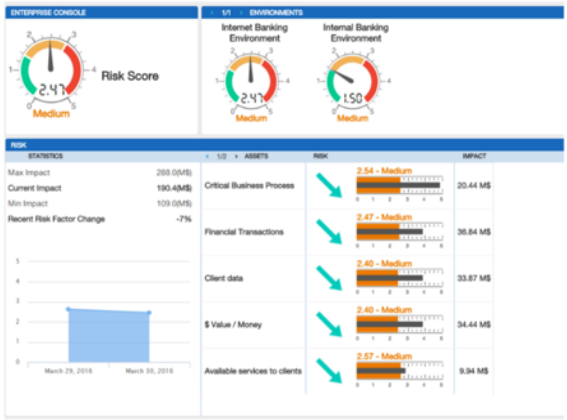


Typical relationship between risk level and financial impact is curvilinear. Reduction of risk from high to moderate yields higher financial gain than reduction of risk from moderate to low.

The end result is that each cell of asset X objective is now populated with the specific financial impact associated with the specific risk score of that cell.

6. Dashboard utilization

The end result of the entire process is the decision support dashboard. At the required level of granularity, the risk officer dashboard consolidates all data into a friendly single pane of glass.



Utilizing this information enables executives to make educated decisions as do risk appetite, resource allocation and risk mitigation by means such as insurance. The risk officer dashboard is extremely important in a what-if scenario simulations - representing expected risk profile inclusive of financial impact enables comparison of apples-to-apples in reviewing alternatives and conducting sensitivity analysis.

About Cytegic

Cytegic provides a full suite of cybersecurity management and decision support solutions that enable CISOs to monitor, measure and manage organizational cybersecurity resources effectively. Cytegic centralizes and consolidates all aspects of cybersecurity risk management: Operations, Decision making, Monitoring, and Reporting, providing CISOs with the tools necessary to become a business enabler.

For further information, please contact Dr. Elon Kaplan, elon.kaplan@cytegic.com