BSC Systems Incorporated

BUSINESS SECURITY RISK EVALUATION

WHITE PAPER

January 25, 2018

The success of various enterprises depends to a large degree on the ability to accurately project stock price performance of the corporations of interest. These enterprises include:

- Stock Brokerages
- Investment Banks
- Venture Capitalists
- Insurance Companies
- Mutual Funds
- Stock and Bond Rating Companies

Typically, the evaluation of a company's stock price has included market analysis, sales projections, competition assessment, and of course financial standing. Certainly, these factors are major drivers of current stock value as well as future performance. However, recent events have shown that a company's stock price can be negatively impacted by security incidents regardless of these traditional predictors. In fact, one study[1] has shown that the price of a victimized corporation declines an average of five percent after an incident. Other studies[2] have found that stock price usually recovers within a year. However, although not focused on stock price *per se*, Ponemon Institute's 2017 Cost of Data Breach Study determined that the average per capita cost of a breach in the United States is $225 per lost record with some industries such as Health Care experiencing a $380 cost. Moreover, this study estimated a probability of 27.7% that a *second* breach would occur within 24 months. According to Ponemon, the effect of a second breach represents a serious erosion in the confidence of both existing as well as prospective customers (customer churn). Regardless, the rate of the victimized company's stock price growth is slower after a security incident than before and the company's stock value lags behind others in its industry for years.[3]

Obviously, organizations that estimate a company's present and future value should include a thorough analysis of risks to the company's sensitive information. Surprisingly, this is not common practice today.

[1] https://www.helpnetsecurity.com/2017/05/16/data-breach-stock-price/

[2] https://hbr.org/2015/03/why-data-breaches-dont-hurt-stock-prices

[3] http://www.techrepublic.com/article/how-a-data-breach-can-negatively-impact-your-companys-stock-price/

So, what should such a security risk assessment include? Here's BSC's approach:

Profiling the Company

Assessing the target company's existing security controls is essential. However, there are three *preliminary* analyses that must be performed; otherwise control assessment can hold limited value and in fact could even be misleading.

1. Sensitive Information Analysis

First, the sensitive information must be identified, characterized and inventoried. The key criterion for identification is whether the loss or corruption of the information could lead to legal action against the company and/or result in loss of business or reputation. Typical categories of sensitive information include Personally Identifiable Information (PII), Protected Health Information (PHI), financial information, classified information, trade secrets, etc. This includes information that is owned by the target company, its customers, or its business partners.

Characterizing the sensitive information involves determining the *degree* of sensitivity. For example, some health-related organizations receive and process only partially or fully aggregated patient health information. These data types must be analyzed to determine if they still fall within the HIPAA definitions for PHI.

Inventorying sensitive information means determining where it is stored – either physically or virtually – how it is processed or transformed in the normal course of business activity, how it flows into and within the company, and how it leaves the company.

2. Boundaries of Responsibility

A direct result of the sensitive inventory exercise is the ability to determine the border at which the company is no longer in control of (and no longer responsible for) the flow of sensitive information. This is normally the interface to an external system with which the company should have a binding agreement to protect the information. However, there are two other "views" of the boundaries of responsibility: physical and human.

Physical boundaries include the spaces within company facilities where sensitive data can be stored or accessed. Today, many companies permit and even rely on mobile workers to access sensitive information. In those cases, the physical boundary must be extended to encompass the types of locations (e.g., home, hotel, etc.) of the mobile workforce.

The company should have a formal list of those positions that are authorized access to the sensitive information. In addition to those positions that work directly with the sensitive data, this list must also identify the IT and management privileged positions that could access the information.

3. Attack Surface

The final step in profiling the company is assessing the number of potential points at which a hacker could gain entry and/or exploit the network. Taken together, these points constitute the company's attack surface. A few of the many examples include:

- The number or Internet-facing web sites that can be used to access sensitive information;
- The use of cloud service providers (CSP) and the allocation of security responsibilities between the CSP and the target;
- The use of mobile devices and Wi-Fi;
- The number and locations of individuals with access;
- The number and geographic dispersion of workstations with access; and,
- The number of subcontractors, vendors and external organizations that have access.

4. Computing the Target Company Profile

Again, these preliminary analyses should be performed without regard to the company's existing or planned security controls. The focus must be on the company's "pure" vulnerability. Only in that way can it be determined which controls are appropriate and, more importantly, to what degree they should be applied.

In accordance with BSC's philosophy of minimum interference with the target organization, BSC obtains the information required for these analyses via an *adaptive* questionnaire. For example, if the answer to the question "Do you use a cloud service provider?" is "no," then the organization will not see the lower level questions that are relevant to cloud usage.

By combining these three dimensions of sensitive information security, an overall company security vulnerability profile can be derived.

Assessing the Security Controls

Usually, the profiling exercise does not place undue interference on the company's staff or operations. The security control assessment is another matter. Recognizing that the target company might view the assessment as both interference as well as a risk to its valuation, careful planning is required to achieve the highest degree of cooperation.

1. Security Assessment Plan

After completing a non-disclosure agreement with the target, BSC will prepare a detailed Security Assessment Plan (SAP) which defines the individual controls that have been selected based upon the target's company profile. These controls must represent the state-of-the-practice and have the highest level of industrial and government acceptance. Today, that control set is defined by the National Institute of Standards and Technology's Special Publication Number

800-53 (NIST SP 800-53).[4] Depending on security impact level (low, moderate, or high), 800-53 specifies up to 212 individual controls. Moreover, some controls are amplified with "enhancements" which can add up to another 173 requirements. The assessor must be intimately familiar with the letter and intent of all of these controls. This, together with BSC's knowledge of the target profile, enables an intelligent selection of applicable controls and enhancements.

The second purpose of the SAP is to specify exactly how each control will be assessed so that the target is fully aware of our expectations. These assessment techniques will include review of security documentation (e.g., policies, plans and procedures), demonstrations of controls (such as log in, session timeout, etc.) and interviews. After delivery of a draft SAP, the target will be afforded the opportunity to digest and obtain clarification for any unclear items. Then, BSC will issue a final SAP that should be signed by an authorized individual at both the target and BSC.

2. Documentation Review

As delineated in the SAP, BSC will formally request the target's existing security documentation including IT policies and procedures (P&P), security plans, employee handbook, security-relevant human resources P&P, etc. If one or more of these artifacts can be released to BSC, their review can be completed at our facility to minimize the time at the target's facilities. Using these artifacts, BSC will complete as many of the control checklist items as possible. This review also allows us to formulate questions which can be forwarded to the target before the site visit. In fact, many of these questions can be discussed and answered via phone conferences prior to the visit. Again, the goal is to minimize time at the target site as well as interference with its operations.

3. Rules of Engagement

If BSC is to perform vulnerability scanning and/or penetration testing, then we will prepare a document known as the "Rules of Engagement" or ROE. This document will include all information recommended by the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment.[5] A full understanding of the boundaries and methods of the scanning is essential to avoid operational and legal issues. Both parties sign the ROE to confirm the agreement.

4. Site Visit

The next task is the actual review of the target facilities that store or process the sensitive information. After sending a detailed agenda, BSC travels to the first site and conducts an in-brief with the CIO or other target company official to review the purpose and bounds of the assessment as specified in the SAP. This is followed by an analysis of each control, recording the following:

---

[4] https://www.nist.gov/publications/protecting-controlled-unclassified-information-nonfederal-information-systems-and-2

[5] https://csrc.nist.gov/publications/detail/sp/800-115/final

- A brief demonstration of the applications or products that process the sensitive information;
- The applicability of the control and, if not, justification for this determination;
- Objective evidence that the control is satisfied (if this has not already been determined prior to the visit);
    - Review of documentation that establishes that the target is executing the control effectively;
    - Review of plans, policies and/or procedures showing that the control is in place or planned;
    - Demonstration of the tools that satisfy controls;
    - Demonstration of the operation of the control (such as two-factor authentication at log in); and,
    - Interviews with subject matter experts to describe the control or other compensating controls that meet the intent.
- A tour of the facility to determine the extent to which the Physical and Environmental controls are met; and,
- Meeting with Human Resources representatives to determine the extent to which Personnel Security controls are satisfied.

BSC will then visit other target facilities which could include data centers, backup data sites, cloud service provider facilities, alternative work sites, etc. The BSC Team then meets to prepare a draft "Findings and Recommendations Memo" which is presented to the target organization's management. The goal is to either obtain agreement with the findings or to gather additional objective evidence for reassessing the finding.

Within two working days, BSC will prepare and deliver to our customer a Risk Evaluation Report that lists the findings and renders our opinion as to the level of risk that the target could experience an incident that impacts the sensitive information.

BSC will continue to support our customer organization should the results of the assessment be disputed in any way by the target company. This is unlikely given that our approach is based upon the most widely-accepted set of security control criteria and that our findings are based on irrefutable objective evidence.