Cyber ROI

A practical approach to quantifying the financial benefits of cybersecurity
Attack
Cyber Investment Challenges

In 2015, global cybersecurity spending is expected to reach an all-time high of $76.9 billion. However, the majority of IT executives anticipate receiving only half of the funding necessary to execute their preferred organizational security strategy. This disconnect is common when it comes to capital planning, but the risk of underfunding cybersecurity defenses has never been greater.

On average, US businesses fall victim to 1.7 successful cyber attacks per week and incur annual costs of $12.7 million to remediate the impacts of these events. The frequency, complexity, and costs associated with attacks is also increasing, with financial damages up nearly 10 percent in the last year alone. Despite these trends, many organizations are reluctant to increase cybersecurity spending because they are unable to accurately quantify the financial value of prospective investments. However, with the right methodology and tools, these organizations can make more calculated cybersecurity investment decisions and channel available funds to address the highest priority security needs.

Pinpointing Needs

Historically, the financial benefits of cyber technology implementation have not been calculated with the same financial discipline used to evaluate other material investments. This was mainly due to a lack of readily available data and systematic methodology to support the efficacy of cyber investments. This gap has prevented managers from being able to formulate generally accepted financial metrics—such as return on investment (ROI), net present value (NPV), and breakeven period—to communicate the value of cybersecurity projects and defend spending decisions.

The path to resolving these challenges begins with the appointment of a Chief Information Security Officer (CISO). The emergence of the CISO role has helped organizations navigate the ever-evolving cybersecurity landscape by ensuring that cyber issues receive proper attention at the most senior level of the enterprise. The CISO provides the vision and functional knowledge to shape an organization’s cybersecurity strategy, establish a cyber budget, and develop controls to protect sensitive information. However, the CISO must also secure funds to carry out the organization’s cyber mission. Without this funding, the benefits of the organization’s cyber functions cannot be realized. It is for this reason that CISOs need a system of tools that can formulate a defensible measure of financial performance, provide sufficient transparency to justify capital allocations toward cyber investment, and operationalize capital planning activities for cyber functions.

Fortunately, the industry has increased efforts to collect, analyze, and publish cyber incident data. Improved access to this information has enabled businesses to advance their understanding of cybersecurity and awareness of the threats and consequences related to cyber breaches. Armed with this new information and the CISO’s leadership, businesses can now develop a standard methodology for quantifying the benefits of cybersecurity investments.

---

An effective cybersecurity investment planning process must be strategic, logical, defensible, and repeatable. A Cyber ROI capability helps CISOs meet all four criteria by providing a standard framework for implementing a cyber investment management system.

The Cyber ROI Solution

An effective cybersecurity investment planning process must be strategic, logical, defensible, and repeatable. A Cyber ROI capability helps CISOs meet all four criteria by providing a standard framework for implementing a cyber investment management system (see Figure 1). When properly applied, the Cyber ROI methodology will quantify the value of cyber investments, produce a robust analytical framework that resonates with an organization’s most senior leaders, increase information transparency to regulatory authorities, and operationalize the cyber capital planning process. There are five key steps to establishing Cyber ROI.

STEP 1: EVALUATE THE VALUE CHAIN

Understanding the enterprise’s existing security framework and how it currently identifies, protects, and responds to cyber threats is an absolutely critical first step in the Cyber ROI process. This establishes the baseline to which all subsequent cyber investment decisions are compared. However, a security framework alone is not sufficient to drive cybersecurity success. Instead, organizations should develop a cyber value chain that accurately reflects both the operating model and core functions of the business. To ensure the approach is holistic, value chain analysis should take both an internal and external perspective, and include activities such as determining key control groups, identifying security gaps, and collecting relevant benchmark data. Trusted industry frameworks, such as the National Institute of Standards and Technology (NIST) and the Federal Information Security Management Act (FISMA), can be used to guide this process, but the final analysis should be customized to account for organizational specifics like industry, size, region, product mix, and the desired state of cyber operations.

STEP 2: ASSESS RELEVANCE AND FUNCTIONAL IMPACT

Once the value chain is clearly established, and security gaps and requirements are understood, the enterprise can begin to address the issue of cyber investment impact. The organization should
start by developing a list of possible cyber projects that address security needs. Each potential project should then be analyzed against the control groups defined within the value chain. Doing so will help assess the incremental functional impact of each potential project and prioritize initiatives for investment analysis.

**STEP 3: QUANTIFY VALUE**

With project parameters defined, the organization can proceed to place a value on each investment opportunity. Many aspects of cyber investment financial value are the same as those for any traditional investment (e.g., costs, benefits, exposure, and risk). The differentiating factor, however, is that cyber investment value is based on three key cost avoidance components: (1) Cost to Fix, (2) Opportunity Cost, and (3) Equity Loss.

**Cost to Fix** — The real costs required to remediate a successful cyber attack. Nearly one in five organizations is expected to experience a cyber breach involving a minimum of 10,000 records within the next 2 years. Thwarting these attacks and their impacts results in a substantial cost avoidance to affected organizations.

**Opportunity Cost** — The potential benefits lost due to a successful cyber attack. In many cases, organizations are significantly hampered or completely shut down by cyber incidents, rendering them unable to operate at normal capacity. Depending on the duration of the event, organizations may experience substantial adverse economic impacts in the form of lost revenue, brand awareness, market position, and even customers. Proper cyber mitigation ensures that the majority of these costs can be avoided.

**Equity Loss** — The direct and indirect capital damages incurred due to a successful cyber attack. Most effective attacks result in the loss of data and/or records. In some instances, this information—such as intellectual capital, trade secrets, or patents—is extremely valuable. Compromise of this information not only inflicts direct harm on the organization, but may also trigger subsequent losses such as declines in market capitalization due to investor response, lawsuits, or leadership turnover. The right mix of cyber investment can protect an organization’s most sensitive information, thus limiting potential equity losses.

When properly applied, the Cyber ROI methodology will quantify the value of cyber investments, produce a robust analytical framework that resonates with an organization’s most senior leaders, increase information transparency to regulatory authorities, and operationalize the cyber capital planning process.

![Figure 2: Expected Loss from Cyber Incidents Calculation](image)
STEP 4: SOCIALIZED FINDINGS

Producing value metrics is without question the most challenging piece of the Cyber ROI process, but delivering actionable information to executives is equally important. In doing so, CISOs help increase awareness of cybersecurity issues throughout the enterprise and establish credibility in defending cyber initiative recommendations to senior leaders. Armed with a set of clear financial metrics, a robust analytical methodology, and hard data to support reasoning, CISOs can clearly articulate the value of cyber projects to decision makers and make a compelling case for increasing investment in cyber initiatives.

STEP 5: INSTITUTIONALIZE THE PROCESS

While Cyber ROI can be deployed as a one-time solution, it should truly be implemented as an ongoing process and integrated with strategic and capital planning activities. Doing so ensures that the organization advances its cybersecurity capabilities and remains a step ahead of threat actors attempting to violate privacy rights and compromise critical information. To achieve this level of adoption and inclusion, it is not only important to formulate...
success. Cyber ROI has helped a CISO of a major infrastructure company achieve a 70 percent increase in budget over 5 years, a healthcare provider justify a single year investment of $53 million to improve the organization’s continuous monitoring capability, and a CISO at a major utility identify targeted investments to reduce end user device risk exposure by 54 percent. With Cyber ROI’s ability to confidently justify, prioritize, and operationalize cyber investment strategies, senior executives can position their organizations to proactively thwart cyber attacks and protect stakeholders’ valued interests.

Guidelines should be established to assign data ownership and document governance and reporting activities. This responsibility should lie with the CISO, but also incorporate relevant stakeholder groups (e.g., data stewards, IT administrators, divisional managers) across the enterprise to foster collaboration and learning. Organizations that follow these recommendations will benefit not only from the analysis and output, but also a set of defined procedures that help frame and inform cyber investment decisions over time.

**Cyber ROI in Practice**

Cyber ROI provides Chief Information Officers (CIO) and CISOs with a methodology and tool to meet pressing cybersecurity needs. Each step in the Cyber ROI process is specifically designed to address a critical component of cyber investment evaluation, starting with value chain analysis and culminating in the implementation of a defined cyber-focused capital planning framework. Most importantly, Cyber ROI is proven in its ability to deliver results. We have deployed Cyber ROI across the spectrum of cyber maturity, often post-breach or after a major cyber incident, with great success.

Each step in the Cyber ROI process is specifically designed to address a critical component of cyber investment evaluation, starting with value chain analysis and culminating in the implementation of a defined cyber-focused capital planning framework.
About Booz Allen
Booz Allen Hamilton has been at the forefront of strategy and technology consulting for more than 100 years. Today, Booz Allen is a leading provider of management consulting, technology, and engineering services to the US government in defense, intelligence, and civil markets, and to major corporations and not-for-profit organizations. In the commercial sector, the firm serves US clients primarily in financial services, healthcare, and energy markets, and international clients primarily in the Middle East.

Booz Allen helps clients achieve success today and address future needs by applying functional expertise spanning consulting, analytics, mission operations, technology, systems development, cybersecurity, engineering, and innovation to design, develop, and implement solutions. The firm’s management consulting heritage is the basis for its unique collaborative culture and operating model, enabling Booz Allen to anticipate needs and opportunities, rapidly deploy talent and resources, and deliver enduring results. Booz Allen helps shape thinking and prepare for future developments in areas of national importance, including cybersecurity, homeland security, healthcare, and information technology.

Booz Allen is headquartered in McLean, Virginia, employs more than 22,000 people, and had revenue of $5.48 billion for the 12 months ended March 31, 2014. Over the past decade, Booz Allen’s high standing as a business and an employer has been recognized by dozens of organizations and publications, including Fortune, Working Mother, Forbes, and G.I. Jobs. More information is available at www.boozallen.com. (NYSE: BAH)

For more information contact:

Fred Blackburn
Executive Vice President
blackburn_fred@bah.com
703-377-8999

Angela Messer
Executive Vice President
messer_angela@bah.com
703-902-5666

Kathryn Kienast
Principal
kienast_kathryn@bah.com
703-377-1314

Contributors:

Leo Simonovich
Lead Associate
simonovich_leo@bah.com
303-881-8792

Stephen Hiser
Lead Associate
hiser_stephen@bah.com
215-990-3970

© 2015 Booz Allen Hamilton, Inc.
C.03.123.15