NABA Recommendation Enterprise Investment in Cybersecurity

Introduction

Determining the appropriate level of investment in an enterprise cybersecurity program is not straightforward. This is due to the fact that the ROI (return on investment) for cybersecurity can be difficult to calculate, as published loss data is difficult to source, verify and relate to current enterprise conditions. It can, in some cases, be less expensive to invest in cybersecurity defences than to pay for the aftermath of a hack, which can include the costs of data restoration, malware mitigation, etc.

Investing in Cybersecurity

Some industries like healthcare, finance and professional services tend to be more risk-averse than broadcasting or the media and as such, will invest more in advanced cybersecurity defenses. Smaller enterprise with less reliance on ecommerce and the retention of personal information tend to be less risk-averse and will invest less. Given that it is difficult to quantify the tangible benefits of such an investment, it should be considered as a form of corporate insurance against the risk of malware, data loss and reputational damage.

Undertaking the process internally, an objective threat-modelling approach to address cyber investment is to:

- Estimate the *financial value of the risk*, specifically the estimated loss over a fiscal year should a cyber security breach occur. There are established formal methods to estimate potential impacts, such as: single loss expectancy; annualized loss expectancy; maximum tolerable outages and recovery time objectives; etc.
- Estimate the *cost and coverage afforded by third-party cybersecurity loss insurance* available on the market that would address this risk;
- Estimate the *cost of investing in augmented, internal cybersecurity defenses* to address the estimated risk.

These steps, taken together, enable both internal and external costs to be estimated, enabling a business-case decision to be taken on the best path forward.

Practical Approaches

In the event internal risk or cost assessments are not possible, there are other options that can be pursued:

Engage a Third-Party Audit Company

To estimate the required investment in an enterprise cybersecurity program, one of the best starting points is to engage a reputable, third-party audit company to perform a thorough assessment. These professionals can be tasked to, as examples:

- Estimate the current level of cyber maturity on a domain basis;
- Work with the enterprise to establish the desired or target level of cyber maturity;
- Identify existing vulnerabilities, their risk profile and relative priority;
- Recommend the additional controls and defenses needed to achieve the target cyber maturity level. Estimate the associated costs;
- Initiate and maintain a risk register to track vulnerabilities, mitigation strategies; timetable, etc. over the long-term.

NABA recommends that the engagement of any third-party audit company be accomplished with a detailed statement of work, a statement of deliverables, audit schedule, payment milestones, remediation steps, etc. to ensure the final audit results fully meet the NABA member's requirements.

Engage an Insurance Company

The insurance industry offers a wide-range of products intended to protect the enterprise's digital assets in the event of a cyber attack, ranging from data breaches to ransomware attacks. While engaging in this process can result in complex and protracted negotiations, it can uncover the key vulnerabilities of the enterprise and potentially the costs to mitigate these cyber risks.

Refer to Trusted Cybersecurity Frameworks

Another approach is to refer to existing, trusted cybersecurity frameworks which are used predominantly in the industry, namely:

- NIST (U.S. National Institute of Standards and Technology) Cybersecurity Framework;
- CIS (Center for Internet Security) Critical Security Controls;
- ISO (International Standards Organization) Frameworks ISO/IEC 27001 and 27002

Each of these frameworks contain a myriad of information on controls, programs and risks and can be used to develop cyber investment plans, depending on the vulnerabilities to be addressed.

Engage an External Cybersecurity Expert on a Temporary Basis

There are certified, freelance cybersecurity experts available in the marketplace, i.e. "CISO's as a Service", who can be leveraged to perform the required cybersecurity analyses, including investment planning. Such expertise can be hired on a time-limited or engagement-limited basis. This approach is particularly attractive to smaller enterprise that might lack the resources to engage a full-time CISO.

Align Corporate Cybersecurity Investment Strategies

With large multi-national enterprise or conglomerate businesses, aligning the cyber investment plans of the various corporate sectors helps to provide a cohesive security strategy. Large corporations typically have dedicated CISO organizations and well-developed cybersecurity policies, guidelines and investment plans.

Don't Be the Most Vulnerable Target

Threat actors will focus on the easiest targets, or the "lowest hanging fruit", like computers, devices, networks, software systems, etc., that are the least protected yet still provide a payback. On-going investments in cybersecurity must therefore take place to ensure the enterprise is more cyber mature than comparable targets.

Recommendation

NABA recommends that its members complete a detailed enterprise threat modelling exercise, using either internal or external resources, to ascertain the appropriate level of investment in cybersecurity for the enterprise in question.

June 17, 2022