An Analytical Framework for Cybersecurity Assessment

Dr. Colonel Gabi Siboni
Founder, G. Bina Ltd.

Cyber threats have become a major problem for every organization. There are many technological solutions, defenses, a lot of advice and many advisors. Before these can be effective, an organization must be able to frame the problem. Specifically, it must understand whether its defenses can mitigate cyber risks, and whether they are effective against existing threats and can provide a means to secure the future. Without such insight, the organization cannot quantitatively assess where investments in cybersecurity should be made. This article describes an analytical framework supporting the security team's and senior leadership's efforts to identify their organization's cyber-threat landscape, determine the appropriate cyber-defense maturity level, and make knowledgeable and prioritized cybersecurity investment decisions. The framework is threat oriented and involves formal best practice risk methodologies.

An Analytical Framework Guiding Cybersecurity Investment

The analysis process consists of four phases: the first two are done in parallel, the latter two are sequential and build upon one another:

- Identify and Map the organization's cyberspace threats;
- Assess the organization's cybersecurity maturity level;
- Analyze the organization's cybersecurity maturity correlated against the threats; and
- Generate a prioritized cybersecurity action and investment plan.

Identifying the organization's cyber threat landscape requires a number of preliminary analyses. The initial step is to determine the Essential Elements of Information (EEI), a statement of the required threat data based on the organization's business activities and requirements. Typically, two domains govern the organization's threat landscape. The internal domain (e.g., vendor vulnerabilities, negligent and malicious employees, management oversights, etc.) and the external domain which includes:

- **The cybercrime space:** Historical analysis of cyberattacks indicates that hacker groups specialize in a specific industry or sector due to the similarity of the IT systems and respective vulnerabilities. Understanding this helps evaluate which threat actors need to be monitored and allows identification of the right sources and forums to monitor in the DarkNet, where most online criminal transactions occur.
- **The cyberwarfare space:** The geopolitical environment in which the organization operates enables identification of relevant bad actors due to their political objectives. For example, a high profile American company may be targeted by anti-American actors such as Russia, China, or ISIS.
- **The ideological space:** Organizations should examine whether their businesses trigger the interest of actors with specific ideological agendas. For example, industrial manufacturing companies with environmental influence should monitor hacktivist groups that support Greenpeace.

Threats are collected from three sources:

- Cyber threat archives and databases such as the IBM X-Force Exchange, the US National Institute of Standards and Technology (NIST), National Vulnerability Database and MITRE's Common Vulnerabilities and Exposures (CVE) database;
- Intelligence collection activity on the Internet and DarkNet;
- Threats previously identified by the organization's security professionals.

These threats are correlated to risks, which are then analyzed to determine their probability of realization and the likely impact on the organization's operations. This process is carried out using threat analysis techniques and results in a ranking of applicable threats with respect to the level of danger posed to the organization.

In a world where organizational budgets are always limited, prioritization of security investments is a critical mission.

The second phase involves analysis of the organization's cybersecurity maturity level. Cybersecurity and information security controls and defenses are evaluated by scoring their effectiveness and assimilation level within the organization and then assigning each an overall control maturity level. Maturity levels can be numerical, e.g., from 1 to 5 with five being the most mature, or descriptive, such as a range between very good and very poor. The cybersecurity maturity level should be visualized in a manner that supports easy information assimilation by senior management. Such visualization techniques include gauge and gumball charts.

Next, controls and defenses that are likely to mitigate each of the identified threats based on best practices and accumulated experience are mapped to specific threats. For example, if a critical threat can be mitigated by a relatively small number of controls, but those controls are at a low maturity level, improving those controls should assume a high priority in terms of time and resources. This analysis can be done manually, but can also lend itself nicely to automation. At the end of this analysis all threats are mapped to controls, providing situational awareness of the organization's defense and mitigation gaps. Additionally, the number of occurrences of each control provides insight into control utility and relative prioritization. This tally is used to provide input into cybersecurity investment decisions.

Finally, after prioritizing corrective measures, the organization determines the resources necessary to address the gaps and to make informed decisions about cybersecurity activities. Using this kind of analytical framework before launching a new product, service, or initiative can also help management understand how the new activity might affect the organization's risk profile and whether it will adversely impact desired cybersecurity maturity levels.

This sort of analysis incorporates cybersecurity principles from the NIST Cybersecurity Framework and standards such as the ISO and the NERC CIP . These principles are combined with cyber security intelligence, threat analysis and the ability of the organization to cope with cyber security threat scenarios to generate a clearly defined way ahead for organizational leadership. Importantly, this is done prior to investment in or implementation of new hardware, software, personnel or programs. As a result, cybersecurity investments are managed quantitatively and effectively.

Summary

In a world where organizational budgets are always limited, prioritization of security investments is a critical mission. Hence, a cybersecurity assessment framework, focused on providing security investment guidance that is the product of quantitative threat and control analysis is an elemental part of cybersecurity capacity building.

About the Author

Dr. Colonel Gabi Siboni *is the Director of Cybersecurity Research at the Tel Aviv University's Institute for National Security Studies (INSS). His consulting firm, G. Bina, provides cybersecurity (ICS and SCADA), Information Technology, ICT & Cloud Risk Management advisory services across Israel and global private sector, including infrastructure and defense firms, as well as most sensitive Israeli government, military and intelligence agencies.*

Dr. Siboni holds a B.Sc. and M.Sc. in engineering from Tel Aviv University and a PhD in Geographic Information Systems from Ben-Gurion University. DSS for Cybersecurity is a G. Bina proprietary methodology and service.

G. Bina
SECURITY Thought Leaders

1. Known also as Intelligence Requests
2. Anonymous supports Greenpeace, hacks oil companies, Patrick Roanhouse, 2012 http://betanews.com/2012/07/16/anonymous-supports-green-peace-hacks-oil-companies
3. The ISO 27000, http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
4. NERC, CIP standards, http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx