BIA, CSF, PCI, HIPAA, CMMC - OH MY!

Ahmed Sharaf
Xband Enterprises, Inc.

If you are like many of us, these are meaningless words without the necessary context.

Unless you've been on a long flight returning from Mars, you're likely not a stranger to the negative impact that cybersecurity or lack thereof is having across the world. The volume, variety, and voracity of cyber-attacks continue to increase while the industry seems to drown itself in acronyms, jargon, and technologies.

Like other industries, it is essential to have a minimum basic appreciation of the language so that your business may effectively navigate the landscape. For industry practitioners, these terms are full of insights that assist with helping to serve their clients, although without understanding drivers of these terminologies, they are effectively useless to the business!

Business owners and Senior leaders struggle with ascertaining risk that is presented to the business. These frameworks, guidelines, and standards help businesses standardize so they may relate in a common language.

A BIA or Business Impact Assessment serves to answer the question, "What are we protecting?" It can also assess how much risk is being presented to the business in financial terms and can serve as a starting point for understanding how to prioritize cybersecurity investments to reduce liability to the business and mitigate financial exposure. At the most basic level the Business Impact Assessment surfaces why and where to invest in cybersecurity so that the business may maximize its investments.

At the higher end of the continuum, a BIA can be very granular when data is combined with a vulnerability scan and using historical data and financially optimized algorithms. This can help a business identify how much financial exposure is associated with a specific vulnerability or type of cyber-attack.

Leavitt Group | XBAND

“With these insights, businesses can utilize this method to help prioritize and strategically discuss their risk exposure, while crafting a plan to mitigate their financial liabilities.”

There are four main strategies available for risk treatment:

1. **Risk reduction**
2. **Risk retention**
3. **Risk avoidance**
4. **Risk transfer**

Performing a Business Impact Assessment helps to quantitatively identify how much risk is presented to the business and how to craft a strategic plan that business owners and senior leaders can review with board members.

Compared to the National Institute of Standards and Technology (NIST), the NIST Cybersecurity Framework serves as a model for international cooperation on strengthening cybersecurity in critical infrastructure, as well as other sectors and communities.

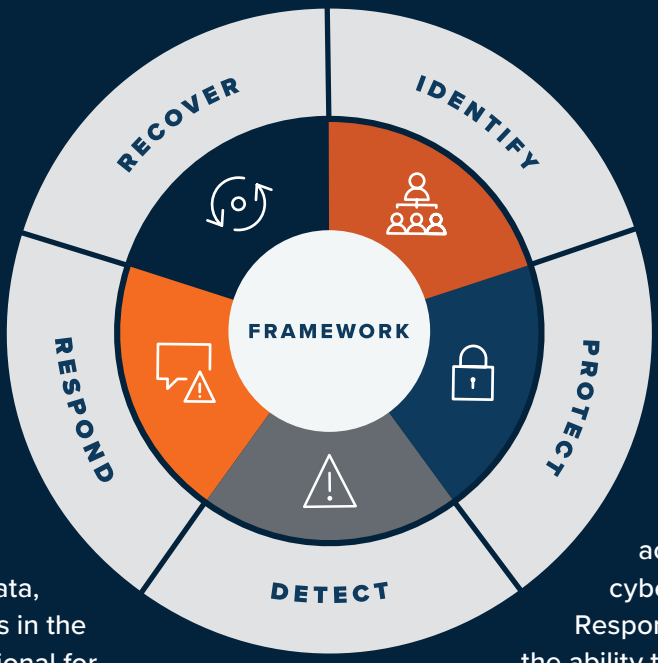
The NIST Cybersecurity Framework (CSF) approach is based on grounded IT security expertise. The guidance is based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk.

In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.

See next page.

Leavitt Group | XBAND

National Institute of Standards & Technology (NIST) Cybersecurity Framework (CSF) Pillars:



Identify – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome categories within this function include Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategy.

Protect – Develop and implement appropriate safeguards to ensure delivery of critical services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome categories within this function include Identity Management and Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology.

Detect – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome categories within this function include Anomalies and Events, Security Continuous Monitoring, and Detection Processes.

Respond – Develop and implement appropriate activities regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome categories within this function include Response Planning, Communications, Analysis, Mitigation, and Improvements.

Recover – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome categories within this function include Recovery Planning, Improvements, and Communications.

Unlike payment card industry standards (PCI), the health insurance portability and accountability act (HIPAA), and the cybersecurity maturity model certification or audit, the NIST CSF guidelines can be utilized across many industries to help reduce risk exposure from cyber-attacks.

Payment Card Industry Standards or PCI are specific to organizations handling or storing Personally Identifiable Information (PII) and engaging in financial transactions.

In contrast, the Health Insurance Portability and Accountability Act or HIPAA and the Cybersecurity Maturity Model Certification (CMMC) are specific to organizations handling or storing healthcare specific data or are related to the Defense Industrial Base (DIB), respectively. Although it is useful, performing a Business Impact or Cybersecurity Framework Assessment does not divest a business from performing a PCI, HIPAA, or CMMC audit if they fall into one of these business segments.

Conclusion

Such frameworks, guidelines, and standards are used as a compass to help navigate the cybersecurity terrain, normalize on a common language, and help mitigate cybersecurity exposure and risk to the business. Engaging with an expert or industry practitioner helps to reduce duplication and "time-to-value," and can position the organization to achieve the desired outcome when working with their insurance partner! XBAND makes the invisible visible and provides actionable intelligence through data powered insights.

Request a no risk business impact assessment, or contact ComTech-Leavitt for a free consultation today!

COMTECH-LEAVITT INSURANCE SERVICES

(800) 211-2508 // comtech@leavitt.com

References

Nist.gov | XBAND

Leavitt Group | XBAND