WHAT YOU NEED TO KNOW ABOUT FOLLOWING CYBERSECURITY FRAMEWORKS

Do you trust what you're eating? I can rest easy; in the U.S., I have the Food and Drug Administration regulating my food supply. Do you trust the product you just purchased? If I I'm in the EU, I have confidence because of the CE mark. Do you trust your bank/supermarket/airline is secure? I shouldn't need to because they follow established security frameworks. This is a long-winded way to say that throughout our lives, we trust regulations and standards to ensure our safety, and cybersecurity is no different. In this blog we are going to look at what security frameworks are, why we need them, how to choose a framework, and, finally, balance things out by looking at the potential downsides of security frameworks.

Why do companies need cybersecurity frameworks?

Short answer: To improve the organization's security posture in the following ways.

- **Standardization:** A common language and set of measures ensures that requirements are well-understood and consistent. Frameworks provide best practices and guidelines that are platform-agnostic to implement cybersecurity measures.
- **Risk management:** A framework provides a structured approach to risk management. It will usually begin with a discovery phase followed by an assessment of the finding. This in turn cascades down into resource (be that time or money) allocation to ensure the most significant threats are mitigated.

- **Compliance requirements:** While many industries have specific regulatory requirements for cybersecurity, non-industry-specific frameworks will align with standards of the regulatory bodies to ensure compliance.
- **Resources/Skills gaps:** Implementing effective cybersecurity controls is no small task. When you add skills shortages (or a complete lack of skills) to the mix, you may wonder where to start. Frameworks offer guidance based on risk, helping to ensure your implementation plan is as effective as possible.
- **Continuous improvements:** The threat landscape is always changing—the next exploit is currently in development somewhere. Frameworks provide the structure to ensure you stay secure and are continuously updated to keep pace with the latest threats for maximum effectiveness.
- **Interoperability:** Similar to standardization but slightly different, cybersecurity measures span the wider digital ecosystem to ensure that collaboration and communication can be facilitated between internal stakeholders and with vendors and auditors.
- **Awareness/Visibility:** The frameworks themselves raise awareness about cybersecurity and promote best practices.

How do you choose a framework?

Depending on your business sector or organizational status, which framework you follow may already be mandated. For example, a company that is publicly traded will need to comply with the Sarbanes-Oxley Act (SOX), so it may use the Control Objectives for Information and Related Technologies (COBIT) framework to achieve this. For US government agencies, the National Institute of Standards and Technology (NIST) regulations must be followed. What if you are not mandated to follow a certain framework? Then you focus on a framework that can help you address one of more of the following:

- Risk:
    - Encompasses risk identification, analysis, evaluation, treatment, and monitoring.
    - Facilitates ongoing monitoring and reporting of compliance efforts.
    - Helps the organization prioritize effort based on risk.
- Control:
    - Provides a high-level strategy for the cybersecurity team.
    - Platform-agnostic set of security controls.
    - Easy-to-digest current state of the organization.
- Program:
    - Covers the whole organization.
    - Assesses the organization's current state in a single place.
    - Measurable.
    - Brings the whole organization into a common language from technical team to executives.

Are there downsides to using a framework?

If a piece of work is improving the security posture, ultimately there is no downside to it, however that doesn't mean it can't be critiqued. There is a common misconception that if you have a followed a security framework, then you are completely secure. While you are better protected than you were before, your security posture must still be validated with assessments and penetration tests

(pentests).

Organizations are complex places, and a one-size-fits-all approach can lead to both over-investment and under-investment in certain areas if they have not been properly risk assessed. While it is expensive to implement a framework, it's also costly to maintain it going forward, which can leave an organization vulnerable if they do not invest in both implementation and continuous maintenance.

Examples of popular frameworks

- NIST CSF (Cyber Security Framework)
- CIS Controls
- ISO/IEC 27001
- Payment Card Industry Data Security Standards (PCI DSS)
- General Data Protection Regulation (GDPR)

Summary

Security frameworks provide organizations with structured guidelines and methodologies that align with industry standards, best practices, and regulatory requirements. Choosing which framework to implement is no small task and requires a significant financial investment and time commitment. Ultimately, adhering to a framework will improve the security posture of the organization, but do not become a victim of a false sense of security. Following the framework alone does not make you secure—you must also conduct security assessments and penetration testing to ensure agility in the face of continuously evolving threats.