Global Knowledge®

Expert Reference Series of White Papers

Cybersecurity Frameworks to Consider for Organization-wide Integration

Cybersecurity Frameworks to Consider for Organization-wide Integration

James Michael Stewart, CISSP, CEHv3-8, CHFIv3-8, Security+, Global Knowledge Instructor

Introduction

A cybersecurity framework is a plan for keeping your data and systems safe. It often addresses an organization's overall security objectives rather than focusing exclusively on just IT elements. Everyone within your organization should make cybersecurity a priority, not just the so-called nerds in the wiring closet. A cybersecurity framework should thoroughly address personnel, networking systems, business computers, portable equipment, operating systems, software, services, business processes, work tasks, communications, data transit, and storage.

Most cybersecurity frameworks are intended to improve the existing security infrastructure already in place. And while many frameworks are crafted or sponsored by governments, this does not mean they can't be applied by other organizations across all industries. A framework can often serve to provide direction, focus, and guidance toward reducing risk, increasing security, improving personnel awareness, reducing downtime, and preventing breaches.

Throughout this white paper we will take a look at common frameworks such as NIST and COBIT, implementation action plans, my framework recommendations, resources for additional information and the government's influence on cybersecurity. First, it might help to take a look at some of the history behind some of our most popular frameworks today.

The Government's Influence on Cybersecurity Frameworks

The National Institute of Standards and Technology (NIST) framework, which is the dominant or most popular cybersecurity framework, came into existence because of government. It is a good starting point though some frameworks predate government initiatives.

In 2013, President Barack Obama issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," which established that "it is the Policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties."

Furthermore the Executive Order calls for the development of a voluntary Cybersecurity Framework that provides a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" to manage cybersecurity risks for those processes, information, and systems directly involved in the delivery of critical infrastructure

services. The framework, developed in collaboration with industry, provides guidance to an organization on managing cybersecurity risks.

To this end, numerous security initiatives have been enacted. These include:

- Office of Management and Budget (OMB)'s Cybersecurity Sprint
- OMB Memorandum M-16-04, "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government"
- Cybersecurity National Action Plan (CNAP)
- CyberCorps: Scholarship for Service program
- National Centers of Academic Excellence in Cyber Defense program
- National Initiative for Cybersecurity Education (NICE) partner agencies
- National Cybersecurity Workforce Framework (Workforce Framework)

This is only a partial list of the new elements that the US government has implemented with the goal of improving our nation's security infrastructure regardless of whether the organization is a government entity or a private company. Some of these programs relate to improving organizational policies, others expand education opportunities, while others improve prevention and response solutions. What these and other government initiatives have in common is a focus on the implementation, adoption, and adherence to a cybersecurity framework. Security is important, attacks are occurring at an increasing rate, and everyone needs to be involved in improving security for our nation, from individuals to corporations to the government and military.

Frameworks Overview

In this section, I provide you with an overview of several important examples of cybersecurity frameworks. This overview can help you to improve your recognition and familiarity with the ubiquity of security frameworks throughout every industry. I recommend that you follow my online references to obtain more detailed information about each framework that seems to address security needs of your organization. Once you find one or more frameworks that are relevant to your security needs, make the effort to integrate them into your security solution.

NIST

The National Institute of Standards and Technology (NIST) Cybersecurity Framework was crafted in direct response to Executive Order 13636 and is based on the existing standards, guidelines, and best security practices already well established in the government, military, and private sector. It was developed in cooperation with numerous private sector security experts and represents a solid perspective on security not just for government agencies and military divisions, but it is also applicable to private sector business as well.

The NIST Cybersecurity Framework is not a detailed checklist to follow and mark off at each stage of completion. Instead, it is a guide for how to assess security, how to consider risk, and how to think about resolving security issues. It is intended to improve decision-making processes and communications about security measures, risks, and breaches. The framework includes instructions for cybersecurity management, communication with both internal and external entities about security issues, improving security planning, and for helping all C-level executives gain awareness about how security affects the organization and how they can make better security-related decisions. It includes recommendations for prioritizing and evaluating investments of time, money, and attention.

The NIST Cybersecurity Framework is based around five core functions of effective cybersecurity:

- Identify
- Protect
- Detect
- Respond
- Recover

The NIST Cybersecurity Framework provides an extensive reference document, which provides information about the sources of the elements of the framework. Following up and accessing these resources is essential for obtaining a full and complete understanding of each element of the framework. The following are some useful links related to the NIST Cybersecurity Framework:

NIST Cybersecurity Framework main site
PWC report, *Why you should adopt the NIST Cybersecurity Framework*
US Computer Readiness Team Program Information

COBIT

Control Objectives for Information and Related Technologies (COBIT) is a security framework for adopting good business practices in relation to IT management, governance, and security. COBIT was crafted by Information Systems Audit and Control Association (ISACA), an international association of professionals focused on IT security governance.

COBIT addresses is designed to assist organizations in re-aligning IT operations with business objectives. There is an assumption that those goals are to improve security, efficiency, and quality of production.

COBIT is based on five key principles of IT governance:

- Meeting stakeholder needs
- Covering the enterprise end-to-end
- Applying a single integrated framework
- Enabling a holistic approach
- Separating governance from management

ISACA provides a wealth of documentation, implementation guides, and other resources to assist in understanding the COBIT framework and integrating it into an organization. A couple of useful links related to the COBIT framework include:

http://www.isaca.org/Cobit/pages/default.aspx
http://www.minimarisk.com/wp-content/uploads/2015/08/Minimarisk_Cobit5_Cheatsheet_v1_0.pdf

ISO/IEC STANDARDS

ISO/IEC 27001:2013 and 27002:2013 are security management standards published by International Standards Organization (ISO) and International Electrotechnical Commission (IEC). These standards originated as a corporate security document from Shell, which were donated to a UK government program in the 1990s. This was then developed into the British Standard BS 7799, then evolved into the ISO/IEC 17799 in 2000, which was

revised in 2005 and 2007, and then reclassified as ISO/IEC 27001 and 27002. The latest full revision was performed in 2013, but amendments were added in 2014 and 2015.

ISO/IEC 27001:2013 defines a formal management system focused on establishing explicit governance over IT security. ISO/IEC 27002:2013 is a high-level security management and implementation guide that recommends best business practices for cybersecurity. These documents address all aspects of an organization, including physical and environmental security, human resource security, access control, asset management, IT security policies, cryptography, operational security, communications security, systems acquisition, interacting with third-parties, incident management, compliance, and more.

The ISO/IEC cybersecurity framework provides suggestions for hundreds of security controls that can be implemented throughout an organization to address any concerns discovered during a thorough risk assessment and evaluation. The guidance also encourages the development of "organizational security standards and effective security management practices . . . to help build confidence in inter-organizational [security] activities." Below are several useful links related to the ISO/IEC cybersecurity framework:

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533
http://www.iso27001security.com/html/27001.html
http://www.iso27001security.com/html/27002.html
http://www.praxiom.com/iso-27001.htm
http://www.praxiom.com/iso-27002.htm

COSO

The Committee of Sponsoring Organizations of the Treadway Commission(COSO) is a joint venture sponsored by five professional associations—the Institute of Management Accountants(IMA), the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), the Institute of Internal Auditors (IIA), and Financial Executives International (FEI)—with the goal of providing leadership guidance to organizations related to overall systems management as well as IT security management. The COSO framework is more about monitoring, auditing, reporting, and maintaining compliance than about designing and implementing a security infrastructure. Thus, COSO is more of a supplement to other security frameworks and not a full security framework on its own.

The COSO framework is based on seventeen internal control principles organized into five groups: control environment, risk assessment, control activities, information & communication, and monitoring. These control principles are to be adjusted for the specifics of an organization and adopted on entity, division, operating unit, or functional basis.

The COSO group provides extensive documentation on their framework, including guides on implementation and references to related materials. Two helpful links related to the COSO framework are:

http://www.coso.org/
https://www.protiviti.com/en-US/Documents/Resource-Guides/Updated-COSO-Internal-Control-Framework-FAQs-Second-Edition-Protiviti.pdf

NERC

The North American Electric Reliability Corporation (NERC) is an oversight group that monitors the electric grid of the United States. NERC is an Electric Reliability Organization (ERO), which means they are responsible for developing and enforcing reliability standards, performing periodic assessments, and educating industry

personnel. To this end they created the NERC 1300 standard, which evolved into the Critical Infrastructure Protection (CIP) standards. The CIP represent a security and operational framework for electric generation, distribution, and management organizations; however, much of their guidance can be adopted by any industry. Here are few valuable links related to the CIP standards framework:

http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
http://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States
http://www.nerc.net/standardsreports/standardssummary.aspx

TC CYBER

The Technical Committee on Cyber Security (TC CYBER) is a subcommittee or division of the European Telecommunications Standards Institute (ETSI). TC CYBER focuses on establishing an international standard for cybersecurity. While they mainly focus on the European Union, their cybersecurity frameworks can be adopted worldwide. TC CYBER is developing standards to increase privacy, improve security for both individuals and organizations, provide security education, provide guidance to manufacturers, and improve security design of products, software, and services.

The TC CYBER standards and framework are freely available online in documents labeled as "TR 103" (Technical Reference) covering a wide range of topics, such as critical security controls, measurement and auditing, service sector implementation, facilitation mechanisms, structured threat information sharing, and personally identifiable information (PII) protection. The following are some useful links related to the TC CYBER cybersecurity framework:

http://www.etsi.org/technologies-clusters/technologies/cyber-security
https://portal.etsi.org/TBSiteMap/CYBER/CyberToR.aspx
http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp1_security.pdf

HITRUST CSF

The Health Information Trust Alliance (HITRUST) is a US-based, privately-held company that developed the Common Security Framework (CSF) in collaboration with experts from the healthcare industry and IT security field. CSF tenets focus on bringing healthcare organizations into compliance with regulations as well as industry standards in regards to organization management and security governance.

Some of the elements of the HITRUST CSF are only applicable to healthcare entities; however, most of its guidance is applicable to everyone, regardless of industry. The CSF integrates U.S. domestic and international standards, regulations, and business requirements, including Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health (HITECH), NIST, ISO, Payment Card Industry (PCI), Federal Trade Commission (FTC), COBIT, and state laws.

CSF addresses adjusting controls based on organizational size, defines clear prescriptive guidance to improve security, uses a risk-based approach to implementing security infrastructure, discusses alternate control options, establishes security as an evolving structure, and assists with achieving and assessing compliance. These two links are related to the HITRUST CSF:

https://hitrustalliance.net/hitrust-csf/
https://blog.varonis.com/theres-something-about-frameworks-a-look-at-hitrusts-csf/

Implementation Action Plan

The most difficult part of integrating a cybersecurity framework into your organization is starting the research. There is no shortcut or substitute for doing your own homework. I recommend designating at least a few hours per framework to read the framework documents themselves as well as look at reviews and evaluations of them. Be sure to seek out both those with positive and negative experiences. Just because a framework sounds good to you, does not mean that it will be a perfect fit for your organization. There are often elements and aspects you did not notice in your initial review. Learn from the concerns of others, and then review the framework documentation a second time.

Unless you are in an industry that has mandatory frameworks that you must stay in compliance with, most cybersecurity frameworks are voluntary. Which also means you can select to integrate some elements from one framework and include other pieces from another security system. The goal is to improve your organization's security infrastructure, not to rigidly apply a system that was not designed with your company specifically in mind.

You will have to adjust any cybersecurity framework to your organization and you will have to adjust your organization to the cybersecurity framework. Keep this in mind throughout the process. You may have to integrate elements in stages over time rather than all at once. The larger the organization, the more challenging it will be to adjust the focus and components of the security system. Also, don't attempt to implement a cybersecurity framework on your own; be sure to obtain senior executive-level permission and include them in the process. Involve all existing IT and security personnel. Then as the adjustments are made, craft updates to employee training and awareness programs to ensure that everyone in the organization is knowledgeable about the refocused security efforts and what their responsibilities are towards the goal of more effective security.

Another concern about implementing a cybersecurity framework is that it is possible that no specific individual framework fits well with your organization. Fortunately, there is no requirement to adopt a framework on an all-or-nothing basis. Thus, you are free to pick and choose the best elements or most applicable components from several existing frameworks in order to assemble your own. This process will not only provide you with a framework customized for your specific organization, but you will also gain a better understanding of the framework concept because you will have to perform deep analysis in order to dissect and reassemble your custom solution.

Here is a summary of the action plan in bulleted form:

- Research the framework options.
- Determine your framework industry requirements or legal obligations.
- Adjust the framework to your organization, while you adjust your organization to the framework.
- Mix and match elements from various frameworks to assemble the best solution for your organization.

Conclusion and Recommendations

No one cybersecurity framework is going to be a perfect fit for any organization. Most of the frameworks I've discussed in this white paper were designed with all industries in mind without customization for specializations. Thus, not everything will apply to every company and not every element will work the same way either.

I hope that this white paper does not serve as another "cool thing of the week" presentation to anyone at the IT worker or senior executive levels. Cybersecurity frameworks are not the fad business concept of 2016.

They are a core organizational improvement concept that needs to be taken seriously and adopted with thought and intention. Keep in mind that each person in your organizational hierarchy will perceive the cybersecurity framework differently, for example:

- Board members may see it as an adjustment of long-term business goals.
- Senior executives may see it as an alteration is business decisions and operational strategies.
- IT executives may see it as a means to improve productivity, while minimizing downtime due to security compromises.
- IT security professionals may see it as a necessary tool to define the security improvements required by the IT infrastructure.
- End users may see it as a change to their daily operational tasks, which results in more secure job functions.

When selecting a cybersecurity framework, consider these and other personnel perspectives within your organization. Ask for input, criticism, feedback, and suggestions on their perceptions of the need for a security framework as well as any specific frameworks up for consideration for adoption. Only with a solid understanding of and a thorough evaluation of cybersecurity frameworks, prior to the attempt to integrate a new security solution, will the process result in successful integration.

The overall goal of security should remain the same: namely protecting your organization's ability to accomplish work tasks while minimizing downtime, data loss, and harm to itself, its employees, and its customers. Security management always requires some core principles to be followed:

1. Always understand what assets you have, need or want to protect.
2. Evaluate the threats that can cause harm to your assets.
3. Consider how much damage or harm could occur if a threat becomes real.
4. Evaluate how often a threat could cause your organization harm.
5. Prioritize your protections based on the biggest harm that could occur the most often.
6. Select protections, countermeasures, safeguards, and security controls that directly address your specific threats and which are cost effective.
7. Never assume the current security stance will always be sufficient.
8. Be flexible and improve security as needed.
9. Keep your employees educated about the need for security and their responsibilities to maintain and enforce security.
10. Stay current on new developments in security defenses as well as new attacks and exploits.
11. Never assume you know everything and that you can't learn from others about security or your own organization's need to improve.

These common-sense security principles should always be the core of any organizational security structure. A cybersecurity framework is a means to fine-tune and improve a company's existing security defenses by using the wisdom and experience of other professionals.

Bibliography

Executive Office of the President. July 12, 2016. "Federal Cybersecurity Workforce Strategy." The White House. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-15.pdf.

Information Systems Audit and Control Association (ISACA). Accessed August 16, 2016. "COBIT 5 Principles." http://www.isaca.org/Knowledge-Center/Academia/Pages/cobit-5-principles.aspx.

National Institute of Standards and Technology. February 12, 2014. "Framework for Improving Critical Infrastructure Cybersecurity." http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

International Standards Organization (ISO) Information Security Management System Requirement and Code of Practice

http://www.iso27001security.com/html/27001.html
http://www.iso.org/iso/catalogue_detail?csnumber=50297

Learn More

Check out the link to Global Knowledge's Cybersecurity Training below to see hundreds of courses that map directly to industry recognized frameworks such as NIST and NICE.

Cybersecurity Training

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

James Michael Stewart has been working with computers and technology for over thirty years. His work focuses on security, certification, and various operating systems. Recently, Michael has been teaching job skill and certification courses, such as CISSP, ethical hacking/penetration testing, computer forensics, and Security+. He is the primary author of *CISSP Study Guide, 6th Edition; CompTIA Security+ Review Guide: SY0-401; Security+ Review Guide, 2nd Edition (SY0-301)*; *CompTIA Security+ Training Kit (Exam SY0-301)*; and *Network Security, Firewalls, and VPNs*.

Michael has also contributed to many other security-focused materials including exam preparation guides, practice exams, DVD video instruction, and courseware. In addition, Michael has co-authored numerous books on other security, certification, and administration topics. He has developed certification courseware and training materials as well as presented these materials in the classroom.

Michael holds a variety of certifications, including: CISSP, CEH, CHFI, and Security+. Michael graduated in 1992 from the University of Texas at Austin with a bachelor's degree in philosophy. Despite his degree, his computer knowledge is self-acquired, based on seat-of-the-pants hands-on "street smarts" experience. You can reach Michael by email at michael@impactonline.com.