EnerNex

DEVELOPING A CYBERSECURITY POLICY ARCHITECTURE

A White Paper

Sandy Bacik, CISSP, CISM, ISSMP, CGEIT

July 2011

620 Mabry Hood Road, Suite 300, Knoxville, TN 37932 // 865-218-4600 (p) // 865-218-8999 (f) // www.enernex.com

INTRODUCTION

In general, policy is a plan or course of action a business intends to influence, determine decisions, actions and other matters and an architecture is the art and science of designing and building something. A cybersecurity policy architecture is the cornerstone of an effective business strategy. Specifically, a cybersecurity policy architecture is the foundation of an enterprise protecting assets, a combination of administrative, technical, and physical protection. A cybersecurity policy architecture needs to be based on executive directives to create an asset protection program, establish protection goals, measures, target and assign responsibilities using the enterprise business mission, vision, and values. The cybersecurity policy architecture development, like a life cycle process, involves the establishment, implementation, monitoring, maintenance, and improvement of enterprise asset production. A cybersecurity policy architecture is an interlocking set of documents that provide guidance for business requirements. This article will form a foundation of what an enterprise needs to consider when developing an effective cybersecurity policy architecture.

WHY THE NEED FOR A CYBERSECURITY POLICY ARCHITECTURE?

The first questions an enterprise often ask in developing a cybersecurity policy architecture are:

- Do we really need a cybersecurity policy architecture?
- How long is this going to take?
- How much staff is it going to take to implement?
- How much maintenance does this requirement?

The goal of a cybersecurity policy architecture is to basically maintain the integrity, confidentiality and availability of enterprise assets and resources. In the absence of an established cybersecurity policy architecture, the enterprise's current and past activities become the *de facto* policy. Without a formal cybersecurity policy architecture on which to defend the enterprise assets, the enterprise may be in greater danger of an asset breach, loss of competitive advantage, customer confidence and government interference. By implementing a cybersecurity policy architecture, the enterprise takes control of its destiny for protecting assets. In the absence of an established cybersecurity policy architecture, the internal and/or external audit staffs and the courts may step in and set protection decisions and internal policy.

When developing a cybersecurity policy architecture, there is a risk in saying too much as there is in saying too little. The cybersecurity policy architecture should provide the asset protection direction required by the enterprise while maintaining discretion in the implementation of the cybersecurity policy architecture. The more details and documents in the cybersecurity policy architecture, the more frequent the update requirements and the more complicated the training process for individuals and third parties. The cyber security policy architecture documents need to be clear and not subject to interpretation on the use, rights, and privileges

of enterprise assets. Individuals need to know what is expected of them and how they will be appraised with respect to using and protecting enterprise assets.

It does not take a long time to write the cybersecurity policy architecture documents, yet the devil is in the details in understanding the enterprise risks and how to protect enterprise assets without greatly impacting operational activities. The implementation and understanding of a cybersecurity policy architecture will be the responsibility of everyone within the enterprise with a core team of cybersecurity experts leading and facilitating the development, maintenance, and implementation of the cybersecurity policy architecture. It is a strong recommendation to create a matrix of topics to be included for the cybersecurity policy architecture; this will limit the repetition of information across multiple documents and limit the amount of time needed for reviews and maintenance. The implementation of a cybersecurity policy architecture may take time, because the individuals need to understand why they need to limit the enterprise asset risk, what it means to them, and how much do they need to change their internal processes to accommodate the implementation of the cybersecurity policy architecture. If the cybersecurity policy architecture is designed and implemented in a business process manner, the enterprise will limit their enterprise asset risk and, possibly, improve individual business processes by uncovering redundancy and information leaks. Once implemented, the cybersecurity policy architecture should be reviewed on an annual basis to ensure the documents continue to fulfill the enterprise and business mission, vision, values, and business requirements.

An enterprise might have technology fail due to the lack of business and cybersecurity requirements when evaluating, purchasing, or developing new technology. Before enterprise technology is implemented, it is important to note that portions of the cybersecurity policy architecture need to be reviewed and updated to ensure the governance and protection of enterprise assets. A good model to think of when looking at the technology and processes within the enterprise is to ensure that any policy architecture documentation is at the center of all business processes, in particular cybersecurity processes, see Figure 1 (Cybersecurity Policy Architecture a Continuous Process).

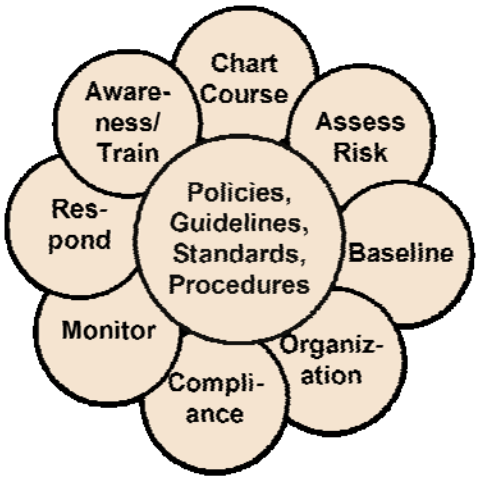

Figure 1 - Cybersecurity Policy Architecture a Continuous Process[1]

WHAT REALLY IS A CYBERSECURITY POLICY ARCHITECTURE?

Simple statements from executive management can have great meaning and value to individuals. The concept of a cybersecurity policy architecture needs to be talked about in the concept of a set of documents and processes for the business. Using a document set concept, the enterprise can supplement their business requirements when divesting or acquiring new entities, evaluating software for implementation, evaluating data flows, or assisting is consequences when someone abuses their privileges within the enterprise. The cybersecurity policy architecture is the enterprise's approach for asset protection and will show the future enterprise your due diligence in protecting enterprise assets. A cybersecurity policy architecture will change, as the enterprise changes and the business requirements change to fit the environment. The cybersecurity policy architecture must compliment the enterprise business model and requirements – do not write a cybersecurity policy architecture for the sake of having documentation.

A cybersecurity policy architecture is a continuous process. It assists the enterprise compliance, risk management, governance, and information assurance and gives the enterprise internal policies, guidelines, standards and processes to monitor enterprise assets. For the most part, the cybersecurity policy architecture is designed to protect critical systems, system owners, system users through physical and virtual controls.

GETTING STARTED WITH A CYBERSECURITY POLICY ARCHITECTURE

When developing or maintaining a cybersecurity policy architecture, the enterprise needs to apply a SMART principle (**S**pecific, **M**easurable, **A**greeable, **R**ealistic, and **T**ime-bound) to ensure

[1] Building an Effective Information Security Policy Architecture, by Sandy Bacik, published by Taylor and Francis Group, page 16, 2008, ISBN: 978-1-4200-5905-2.

the cybersecurity policy architecture continues to meet the enterprise business requirements. All enterprise documents should have a defined scope, how much or how far does the document encompass. For the most part, a cybersecurity policy architecture includes anyone and anything that connects to, communicates with, or accesses an enterprise asset. When developing a cybersecurity policy architecture it is important to note that the documents should:

- Be easy to understand
- Be applicable to the enterprise environment
- Be enforceable and do-able
- Be phased in or staged for implementation
- Meet business objectives.

Depending upon the enterprise culture, the enterprise individuals will need to understand how the cybersecurity policy architecture fits into the enterprise architecture. By performing a business link with the enterprise value of assets can assist in developing support for the cybersecurity policy architecture, something similar to the Figure 2 (Connecting with Enterprise Values) below.

Figure 2 - Connecting with Enterprise Values[2]

A basic process that is followed when developing documents within the cybersecurity policy architecture can be seen in Figure 3 (Cybersecurity Policy Architecture Development Process). It is normally an event, incident, requirement, or some sort of request that initiates the process for developing or modifying a document within the cybersecurity policy architecture.

[2] Building an Effective Information Security Policy Architecture, by Sandy Bacik, published by Taylor and Francis Group, page 125, 2008, ISBN: 978-1-4200-5905-2.

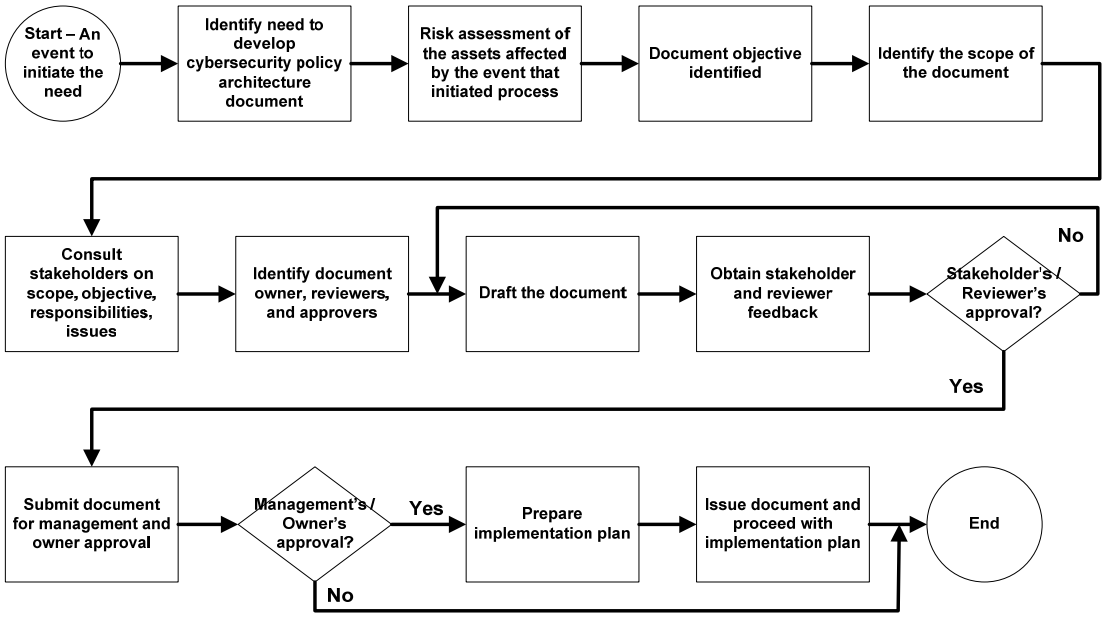

Figure 3 - Cybersecurity Policy Architecture Development Process

The cybersecurity policy architecture should be written to clear up confusion, not generate new issues. Remember the reading and comprehension level of the enterprise individual and when writing the documents, remember the 5 Ws of Journalism 101:

- What - what is to be protected (the Intent)
- Who - who is responsible (Responsibilities)
- Where - where within the organization does the policy reach (Scope)
- How - How will compliance be monitored (Compliance)
- When - when does the policy take effect
- Why - why was the policy developed

If you use a topic based approach to the enterprise cybersecurity policy architecture, many components may already have been written and just need to be enhanced and centrally located. And when writing, if the lower level document relate to a higher level enterprise document, then the minimal number of documents will need to be written, see Figure 4 (Laying Out a Policy Architecture).

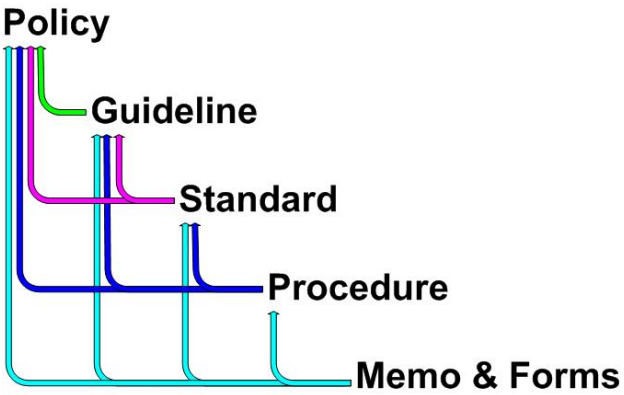

Figure 4- Laying Out a Policy Architecture[3]

The enterprise also needs a basic set of document definitions, if they have not already been defined, for a cybersecurity policy architecture, such as the following Table 1 (Sample Definitions).

Consultant	An entity that provides expert or professional advice.
Contractor	An entity that performs services for another person under an express or implied agreement.
Customer / Client	An entity that buys goods or services.
Employee	An entity that is hired by the enterprise.
Guideline	An outline for a statement of conduct. This is a guide as to how something or something should perform, such as acceptable use of the Internet.
Partner	An entity that is associated with the enterprise in performing activities from a non-enterprise facility using a non-enterprise infrastructure.
Policy	A high-level statement for goals/behaviors/consequences
Procedure/Process/ Work Instruction	Documented step-by-step instructions to get to a goal
Staff	Any entity that falls into the categories of Client, Consultant, Contractor (PO), Contractor (regular), Co-Op, Customer, Employee, Partner, Student, Vendor, or Volunteer.
Standard	A standard set of rules and procedures that are required
Vendor	A seller. One who disposes of a thing in consideration of money.

Table 1 - Sample Definitions

[3] Building an Effective Information Security Policy Architecture, by Sandy Bacik, published by Taylor and Francis Group, page 25, 2008, ISBN: 978-1-4200-5905-2.

A simple initial list of cybersecurity policy architecture topics includes the following:

Certification of systems and applications

Chain of trust and partner agreement

Record Processing

- Release of Information
- Confidentiality Agreements

Access control

- Access authorization, establishment, modification – network
- Access authorization, establishment, modification – email
- Request for account enable/disable/unlock
- Request for UserID & Password

Security configuration management

- Change Control
- Configuration Control
- Inventory (owned, leased, loaned)
- Operating system
- Application
- Hardware
- Inventory
- Anti-virus
- Encryption (if used)
- Security Testing

Security management process

- Security Policy
- Risk Analysis & Management
- Assigned security responsibility

Media controls

- Accountability / access control (Liability Agreements)
- Backups
- Data storage
- Disposal

Physical access controls

- Verify access prior to physical access
- Visitor logs / escorting
- Hard keys
- Key card
- Testing and revisions
- Need to have/know access
- Secure workstation location

Security awareness training

Access control

- Audit controls
- System banners
- Access control lists
- Authentication
- Audit configurations
- Logs

Authorization control

- Request for UserID and System Access (content, user, or role-based)
- Role based authentication
- Data authentication
- Entity authentication

Communications/network controls

- Banners
- Access controls
- Alarm
- Audit trails
- Encryption (optional)
- Entity authentication
- Event reporting
- Integrity controls
- Message authentication
- Software Use
- Modem Use
- Internet and E-Mail Usage
- Classification of Information

Once there is an initial list of topics and the enterprise knows what existing standards, legal and regulatory requirements are required, and then a matrix for easier maintenance can be established, such as the Table 2 (Cybersecurity Policy Architecture Compliance) below.

Enterprise Area	NISTIR 7628 v1.0	ISO 17799	PCI DSS	EU Privacy	CobIT	Common Criteria	Generally Accepted Privacy Principles	Generally Accepted Security Principles
Access Control	X	X	X	X	X	X	X	X
Application Development	X	X		X	X	X		X
Asset Management	X	X	X	X				X
Business Operations		X	X	X	X	X	X	
Communications	X	X	X	X	X	X	X	X
Compliance		X	X	X	X			
Corporate Governance	X	X		X	X			
Customers	X	X	X	X	X		X	X
Incident Management	X	X	X	X	X	X	X	X
IT Operations	X	X	X	X	X	X	X	X
Outsourcing		X	X	X	X	X	X	X
Physical / Environmental		X				X		X
Policies & Procedures	X	X	X	X	X	X	X	X
Privacy	X	X	X	X			X	
Security	X	X	X	X	X	X		X

Table 2 - Cybersecurity Policy Architecture Compliance

MAINTENANCE OF A CYBERSECURITY POLICY ARCHITECTURE

As stated previous, all documents within the cybersecurity policy architecture should be reviewed on an annual basis. An annual review does not mean the cybersecurity policy architecture documents require updates annual, it is to ensure that cybersecurity policy architecture remains current and in alignment with the enterprise business requirements. A simple matrix to help who is the owner, the reviewers, and the last review of each cybersecurity policy architecture document can be seen below in Table 3 (Cybersecurity Architecture Maintenance Matrix). Performing an annual review and maintaining a matrix will assist and limit the time necessary for regulators and auditors when performing testing and compliance tasks. Adding another column of 'location' will also allow the review to know exactly where the most current copy of the cybersecurity policy architecture document resides for efficient access.

Document	Description	Document Number	Owner	Reviewers	Approved	Date Last Reviewed	Date Published	Comment
Incident Handling Procedure	Describes the process for investigating an electronic incident.	IN005037	CSO	IT Ops, IT Mgt	Yes	2009/08	2009/08	IT Approved
Incident Handling Standard	Describes standards used when investigating an electronic incident.	IN005036	CSO	IT Ops, IT Mgt	Yes	2009/08	2009/08	IT Approved
Information Assurance Policy	Describes the over arching stance on information assurance within MYC.	MS005856	CSO	IT Mgt, VP HR, VP IT, CFO, VP Global Ops, CEO	No, but approved within IT			HR, IT approved 07/09; Waiting since 07/20/06 for CFO and CEO approvals
Information Security Program	Describes the tasks and responsibilities of the information assurance program as it relates to the enterprise	SA005005	CSO	IT Mgt	No, but approved within IT			HR, IT approved 07/09; Waiting since 07/20/06 for CFO and CEO approvals
IT Change Control Process	This process addresses a consistent method used to assess, coordinate, and carry out all modifications made to the IT Infrastructure.	PD005420	IT Mgt	IT Ops, IT Apps, IT Mgt	Yes	2009/08	2009/08	IT Approved

Table 3 - Cybersecurity Policy Architecture Maintenance Matrix

While the development and review of a cybersecurity policy architecture is similar to a development lifecycle, the cybersecurity policy architecture continues to evolve as the enterprise grows. The enterprise can look at the cybersecurity policy architecture in Figure 5 (Cybersecurity Policy Architecture Lifecycle) for servicing the enterprise's cybersecurity policy architecture.

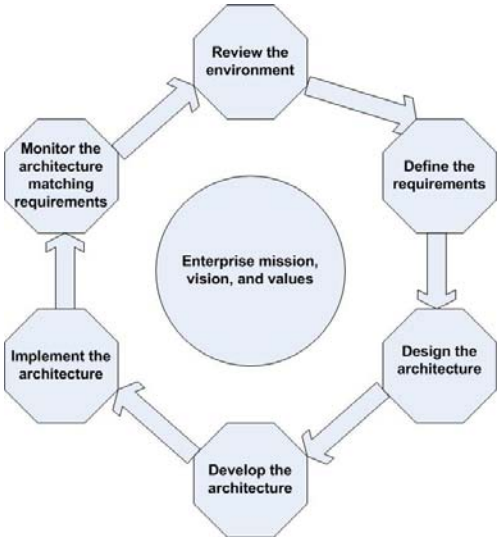

Figure 5 – Cybersecurity Policy Architecture Lifecycle[4]

CONCLUSION

Most enterprises would prefer to establish their own cybersecurity policy architecture instead of having some third party impose internal protection. The basic threats that may prevent an enterprise from reaching this goal are unauthorized access, modification, disclosure or destruction, whether deliberate or accidental, of the information or the systems and applications that process and use assets. A cybersecurity policy architecture documents the enterprise's ability to protect assets against risks and threats. The cybersecurity policy architecture also coordinates the enterprise's lines of business, looking at the risk, balancing it with protection enterprise assets, regulatory and business requirements. The enforcement of a cybersecurity policy architecture will be through a combination of administrative and technical procedures and processes.

When a cybersecurity policy architecture is integrated into an enterprise development, product, and security lifecycle, the risk and threats to enterprise assets is limited and compliance and governance of those enterprise assets will be integrated into all business

[4] Building an Effective Information Security Policy Architecture, by Sandy Bacik, published by Taylor and Francis Group, page 150, 2008, ISBN: 978-1-4200-5905-2.

processes making cybersecurity everyone's responsibility and remember a few things about good documents:

Getting Accurate Info	Good documentation is accurate and assists the enterprise in protecting assets.
Obtaining Details	Ask follow up questions such as who, what, when, where, why, and how.
Operations	Operating processes cannot be greatly impacted.
Documenting Problem Summary	Ensure it is know what issues are being solved through asset protection
Documenting Details	Be specific when writing the more detailed documents of a cybersecurity policy architecture, such as standards and procedures.
Only	Only keep to the subject of cybersecurity and asset protection.
Changes	Document changes to the enterprise environment and documents.
Understanding	Ensure the cybersecurity policy architecture documents are understood by all entities.
Everyone	Everyone in the enterprise needs to be included in the cybersecurity policy architecture implementation.
Network	Network with all levels of the enterprise to ensure an understanding of the need for a cyber security policy architecture.
Total Enterprise	All assets within the enterprise need to be included within the cybersecurity policy architecture.
Satisfied Enterprise	Through monitoring and active participation in implementing and maintaining a cybersecurity policy architecture, the enterprise can limit the risk to assets and be satisfied with the asset governance.

ABOUT THE AUTHOR

Sandy Bacik, EnerNex Principal Consultant, author and former CSO, has over 15 years direct cybersecurity development, implementation, and management experience in the areas of Audit Management, Disaster Recovery/Business continuity, Incident investigation, Physical security, Privacy, Regulatory compliance, Standard Operating Policies/Procedures, and Data Center Operations and Management. Ms. Bacik has managed, architected and implemented comprehensive information assurance programs and managed internal, external, and contracted/outsourced information technology audits to ensure various regulatory compliance for state and local government entities and Fortune 200 companies. She has developed methodologies for risk assessments, information technology audits, vulnerability assessments, security policy and practice writing, incident response, and disaster recovery. Ms. Bacik currently volunteers and co-chairs subgroups with NERC, NIST, and UCA OpenSG; assists in developing interoperability and security standards and requirements for the Smart Grid. Ms. Bacik is the author of *Building an Effective Security Policy Architecture* (2008) and *HIPAA Security by Example* (2012) and a contributing author to the *Information Security Management Handbook* (2009, 2010, 2011, 2012).