The Security Trifecta

IT Security Governance Demystified

Let's begin with one simple undisputable fact about information security; we are all in the same boat! Information security must evolve just as information security challenges or threats evolve. Cyberspace criminals are becoming more organized, more educated, and more brazen in their pursuits. Once our market place consisted of what were predominately localized transactions and interactions. Now everything has changed.

We conduct business with our partners from anywhere around the globe thanks to digital communication networks.

This article is focused on helping you understand the fundamental elements that an IT security governance program should have in place. I'll also expound a bit and include some of the governance supporting functions to help illustrate how IT security governance would be integrated within your corporate IT security department.

As with any endeavor in this life, our risk exposure potential increases exponentially with our increase in these activities. Not that taking risks is bad or that increasing our potential exposure is a negative thing, on the contrary! We increase our opportunities and potential by taking risks. The best approach is one that is well informed and with our eyes wide open.

The Internet was conceived with the intention of making communications and transactions easier; mission accomplished. To many people, the Internet and Internetworking appear to be totally open without controls and without consequences. It is as if the world no longer had countries, borders, or boundaries in place to enforce a local set of standards for its citizens.

The reality is quite different. Our networks, even Darknets, are all built on systems of control. They all have boundaries. We have the ability to enforce these controls between a state of no control and total control. We establish control to eliminate risks and to facilitate opportunities.

When considering risks, these come in the form of human conduct and technological malfunctions. The technological facet consists entirely of technological applications that break down for some reason or that is out of our control and ability to predict.

The human element is by far the most dynamic but also the easiest to predict. There are some fundamental attributes to consider when you examine this challenge.

Just like we see in American police shows where the criminals have the means, the motive, and the opportunity (MMO) of the individual.

For example, cyber-criminals are increasingly sponsored by governments or criminal organizations now. Under this situation, criminals are provided with the resources, or means, they need to wage cyber-attacks against some external entity.

Where once the motives of hackers was notoriety, now they are more for profit, hacktivism and espionage. Cyber-crime and Cyber-espionage has become a business and no longer a novelty pursuit for the technologically talented.

Let's review these common motivators

Espionage

This has become a state supported and a corporation supported practice without visible repercussions or penalties. Intellectual property is stolen by companies devastating business value. Governments destroy critical infrastructure or subvert the sovereignty of other nations.

Financial Gain

The theft of human identities and financial data has led to epic economic damage. Our trust in financial organizations, security practitioners, security products and security services is in question with good reason.

Hacktivism

The more random element is in hacktivism. There are some really great cases where exposing the truth brings positive changes to the world. We have also seen instances that more resemble anarchy than the more noble cause.

The Security Trifecta

There is a way forward to a successful cyber defense. At a high level, it is crucial we apply a three phased approach through *governance, technological enforcement,* and *vigilance* to security. I've referred to this approach as The Security Trifecta in my books and publications to raise awareness on a sustainable and fundamental process to reduce cyber threats to your organizations.

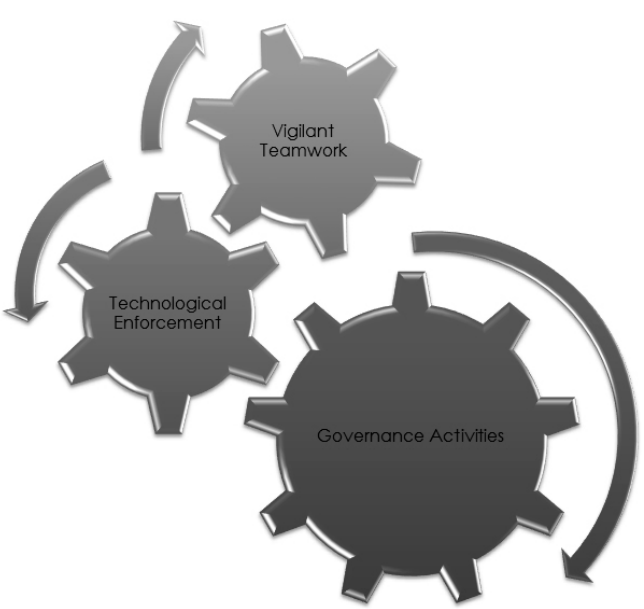


Figure 1. *Security Trifecta Scheme*

- Governance: We set standards through governance. Rules, laws, processes, and procedures set the framework for our success.
- Technology: We enforce our governance through technological controls.
- Vigilance: We test; we refine; and we monitor our cyber defense programs vigilantly always working to maintain our edge.

Without order, we have disorder; the opportunity for these events to occur increases exponentially with the complexity of our technology systems, networks, and applications we implement. This condition is exacerbated when the same systems fundamental underpinnings are not maintained adequately. New threats are being discovered regularly and new countermeasures are keeping pace; but only if we maintain these countermeasures.

So what exactly are some of the challenges we are faced with as security practitioners? Only until very recently, information security was considered by most to be just a niche profession or technological process. This scenario has changed completely in just the past ten years.

Information security had been the realm of Chief No Way Officers and other security technologists who only offered barriers to business. The reality is that information security must be transformed into a business enabler instead of the business inhibitor it has the reputation be being. What do we need to do within our organizations to change this negative situation and turn it into something with positive business value?

We get there when we enable business by eliminating risks to business. We get there by eliminating the threats to the line of business. As security practitioners, we must be creative and agile in our professions to identify opportunities for improving the overall security posture we are diligently striving for. We must also understand the language of our customers regardless if they are outside of the company or employees of our company. They have a job just like we have a job to do and when we take the time to understand that, when we take the time to listen effectively, we put ourselves into a position to do the most good and to be more effective at removing those business barriers. Only when we achieve success in this space will we be able to move forward and advance our information security mission.

The very heart and soul of The Security Trifecta are three distinct facets we will explore together.

Those three well defined pragmatic steps I mentioned earlier are Governance, Technology, and Vigilance. Without order, we have disorder right? How do we begin implementing order from the technological chaos many of our corporate infrastructures are made of?

Top Down Governance

Through *Governance* activities which is the written word, the law, or policies and procedures! Information technology and security policies hold a special place within the enterprise. Just like our technological implementations have risen to importance supporting the majority of our business processes today, the obvious need for standards, policies, and controls has become obvious.

It might seem that the definition you use to describe the particular governance document does not really matter, but you would be mistaken. While generically referring to all governance documents as policies is fine, the actual textual descriptions are very important. The reason for this need for specificity hinges primarily on regulatory taxonomy. Policies will be viewed as concrete directives whereas standards are more transitive. You must strike a balance between maximizing security, risk management, and meeting regulatory requirements, while minimizing business impact.

External Regulations within the context of this publication refer to any external legislative mandate, regulatory obligation, and industry requirement facing the organization. Examples are Sarbanes-Oxley (SOX), Payment Card Industries Data Security Standard (PCI DSS), Federal Information Security Management Act (FISMA), UK Data Protection Act, or the Data Protection Act (India) are just a few examples of the plethora of regulations potentially facing your organization.

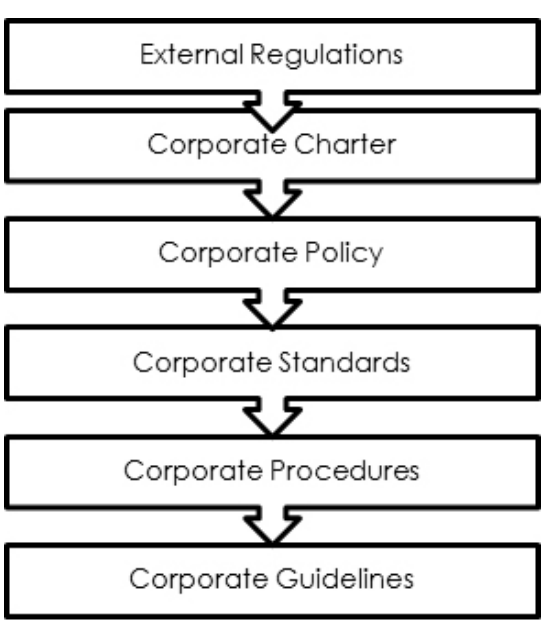


Figure 2. *External Regulations hierarchy*

The most prudent first step in determining which external regulations are applicable to your organization would be to consult the General Counsel if your company has one or consult with an attorney who specializes in Federal and International cyberspace law. There is inner-state, intra-state, federal, international, cross-border, and specific country laws and regulations to adhere to. Keep your facts straight to prevent any unwanted consequences from occurring.

The *Corporate Charter* for information technology and security serves as the capstone document for the Information Security Program. The Information security charter defines how the organization approaches security and if a governance framework will define the trajectory of the complete set of information technology and security governance documents. This of course sets the foundation for the technical controls, monitoring, testing, and ongoing pace for the entire security program.

Choose wisely and ensure that whatever framework you select, it is comprehensive. There are logically seven overarching topical areas applicable to Information Security. First, there is the asset identification and classification category, second, the asset protection category, third, the asset management category, fourth, the acceptable use category, fifth, the vulnerability assessment and management category, sixth, the threat assessment and monitoring category, and finally, the security awareness category. *Corporate Policies* are specifically used to establish the holistic requirements and guiding principle used to set direction in an organization. They can be a course of action to guide and influence decisions. Policies should be used as a guide to decision making under a given set of circumstances within the framework of objectives, goals and management philosophies as determined by senior management. An example of this would be that your comprehensive information technology and security program include the holistic set of controls covering asset identification and classification, asset protection, asset monitoring, asset management, acceptable use, vulnerability assessment and management, threat assessment and monitoring, and security awareness.

Corporate Standards are specifically used to define some of the overarching specifics mandated by the higher-level policies. They are used to establish normal operations or requirements as they apply toward technology-based systems. Information Security standards provide more measurable guidance in each policy area. They establish uniform engineering or technical criteria, methods, processes and practices. A standard may also be used as a controlling artifact or similar formal means used to establish evidence of review activities, governance expectations, compliance requirements, and other regulating activities included in your information technology and security governance program. An example of a standard would be defining the encryption cipher strength permitted for corporate business applications as defined by the encryption standard.

Corporate Procedures or guidelines are specifically used to articulate in great detail the steps, configuration specifics, and production requirements necessary in the designated usage of corporate information assets and business applications. Information Security procedures describe how to implement the standards. An example would be that employees should not cite or reference clients, partners or suppliers without their approval. When you do make a reference, where possible, link back to the source as required by the companies Social Computing Guidelines governance document.

With the explosion of a plethora of technological permutations touching every aspect of our life and business activities driving this change, so too must the bedrock of our governance activities remain agile as well. Without order, we have disorder. Rules must be established so boundaries remain defined. The rules of the road were established to keep us safe so that we arrive alive.

Other facets of our lives have rules in force that help increase efficiency, decrease risk potentials, increase accountability and protect the innocent. The logical conclusion from a technological standpoint is that governance activities are vital to our success.

The single biggest problem facing corporate information security can be directly traced back to the lack of well-defined corporate information technology and security governance documents. This is in part what I wrote about in my recent book, *Governance Documentation and IT Security Policies Demystified*. It establishes the baseline for everything we are trying to do.

At the very top of the governance structure you must set the pace for everything else that follows. With the Internet, we are all members of international organizations. Think like an international organization and begin with an international standard such as the ISO 27001 and ISO 27002 information security standards.

The key to a successful security program begins with the top of the organization and works its way down to the entry-level employees. This top down approach ensures your success. For example, if the CEO of the company refused to abide by the password policy the company established, why would anyone expect the entire organization to abide by the rules? Senior leadership must set the tone for the company and set the example. There should be no room for compromise. The alternative is a breakdown of command and control leading toward vulnerabilities, risks, and potential company damage that might not be repairable. The same approach is equally effective when we are working with the

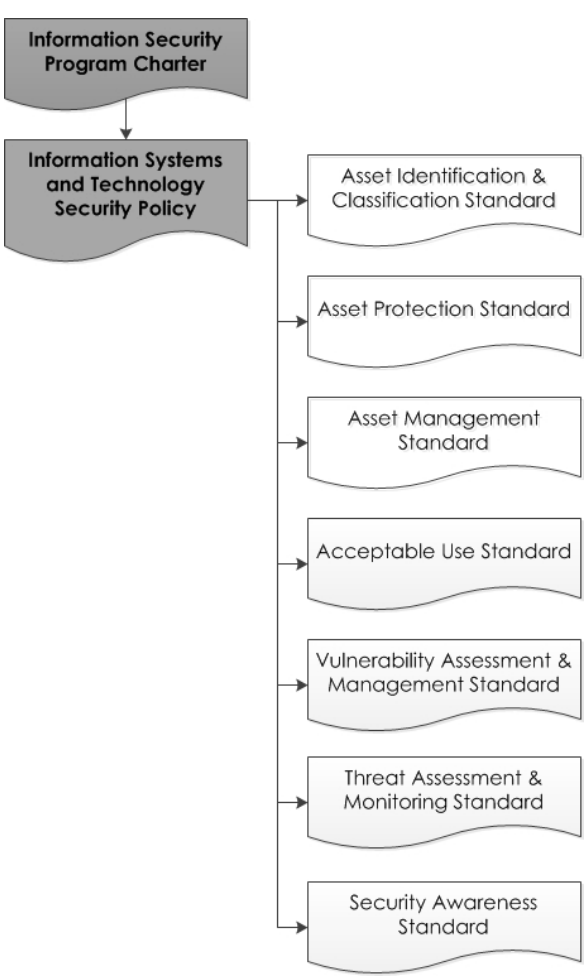


Figure 3. *Informations Security Program Charter*

organizations governance documentation. There must be a logical hierarchical framework distilled from the distinctive facets of technology implemented, its usage, and its management (Figure 3).

We all know by now that our security efforts will generally fail without the support of senior management. The same top down principle applies to our governance documentation and program. At the very top level, we need to set the tone for everything that follows. A corporate IT security charter and IT security policy accomplishes this need. From there we make the decision to model our standards after a particular security framework or standard. What I'm going to share with you right now is a deeper dive into the distinct facets of a holistically applied governance program.

Asset Identification and Classification

The Asset Identification and Classification category that defines company objectives for establishing specific standards on the identification, classification, and labeling of company information assets (Figure 4).

You must know where you are going in order to get there efficiently. You need to discover what your critical assets are, what their value is, and how to rank their priority for protection before you do anything else.

For example, *confidentiality* classifications are important so that information is not improperly handled. You may have company information and intellectual property that would be restricted access, or confidential access, or internal use only, and even publicly available information classifications. By determining up front what your information classifications are, you will get a better idea on what protective measures are required.

We all like names don't we? Once you have decided how to classify something, make sure a label of some form is attached to it. This might be a physical tag or it might be an electronic tag. In either situation, it provides a mechanism to manage your business assets through the use of technology or process.

Consider date *integrity* for a moment. When sharing information or transmitting information which could be in the form of a business transaction or simple file transfer to another person. How do you ensure that your data is not corrupted or tampered with by another person? There are encryption and other data tampering protective technologies available today to help with integrity.

Let's consider data *availability*. Information is useless if it is not accessible to the people it is intended for. When you ranked the importance of your information assets, you decided how critical it is to make it available. Maybe something is so

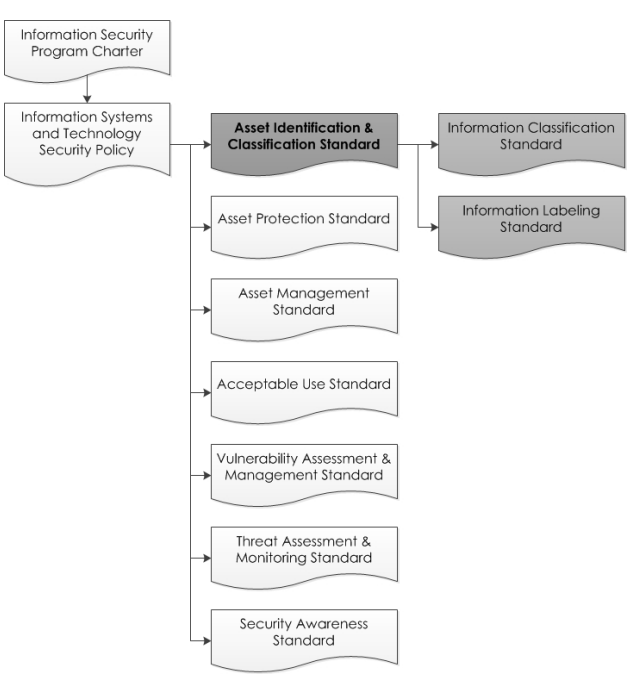


Figure 4. *Asset Indentification and Classification Standard*

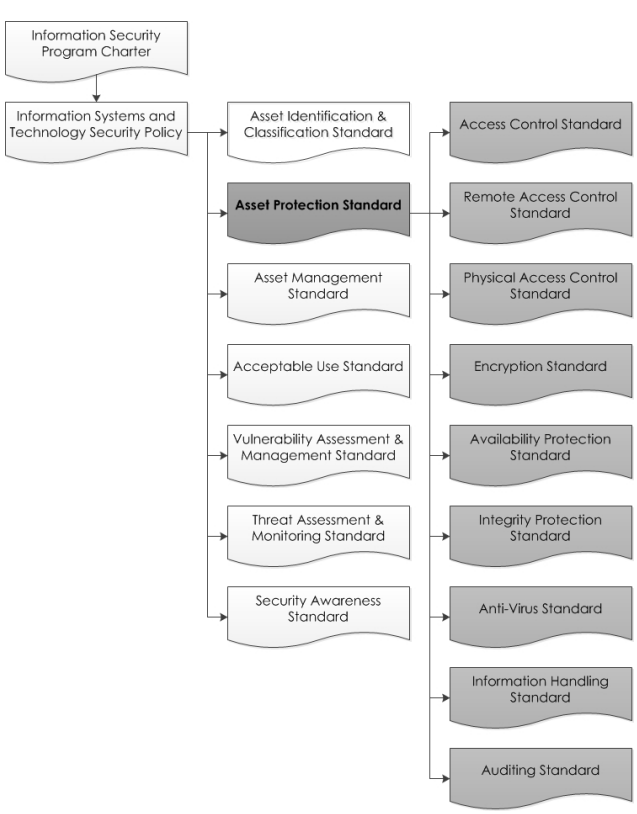


Figure 5. *Asset Protection Standard*

valuable that you cannot afford to have it offline for an extended period of time. These factors will go into your decisions.

Asset Protection

The Asset Protection category defines the company objectives for establishing specific standards on the protection of the confidentiality, integrity, and availability of company information assets I just mentioned (Figure 5). There are several asset protection facets to consider. For example, access control standards provide specific instructions and requirements for the proper identification, authentication, and authorization controls necessary to access company information assets. Both physical access and electronic access must be considered. When protecting electronic assets, encryption is a necessity. An encryption standard will provide specific instructions and requirements for the encryption of sensitive information assets to your enterprise. Disaster recovery and business continuity standards will be used to define how the availability and integrity facets of the asset protection needs of your organization are defined. Anti-virus and malware protective standards will all help to define the standard you intend on utilizing to again, protect those valuable corporate assets. Part of asset protection involves implementing the controls over your information classification and labeling exercise with information handling standards. All of these controls I've mentioned require oversight and testing so establishing our auditing control standards over our asset protection efforts is essential.

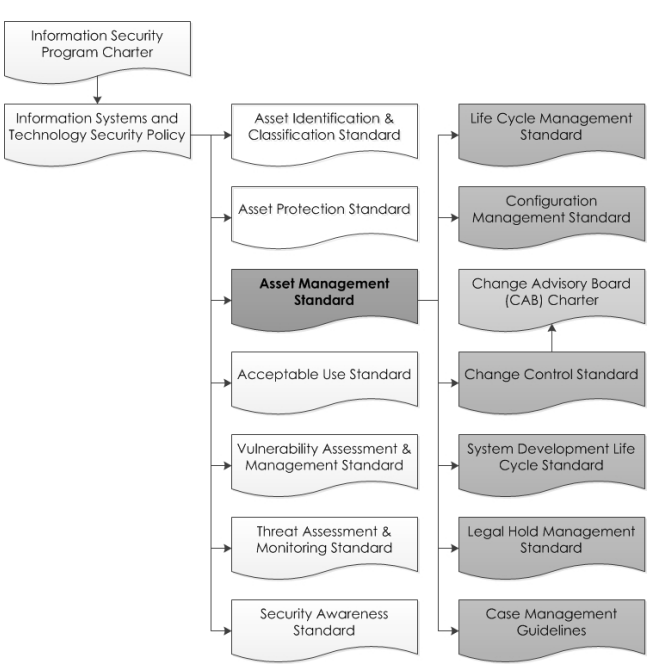


Figure 6. *Asset Protection chart*

Asset Management

The Asset Management category defines company objectives for establishing specific standards for the management of the networks, systems, and applications that store, process and transmit company information assets (Figure 6).

We are now looking at a whole batch of activities revolving around controlling configurations of the technology controls you have implemented already. The enemy to operational stability and information security is effectively changed. Not that change is a bad thing, quite the contrary, but we must be aware of the challenges it brings so that change is managed effectively.

Change will most often be associated with software or system development life cycles. Consider the implications for a moment. If you develop software or deploy new technology, it all introduces new benefits and new challenges.

We all know by now that not updating software might benefit operational stability, but we also know that software bugs and security vulnerabilities are discovered that negatively affect operational stability. During your risk assessment, you identified business assets and placed a value on them. You could take annualized loss expectancy, otherwise known as ALE, and place a tangible cost to doing something about it or doing nothing about it. Maybe your solution comes in the form of a compensating control instead. The second step is identifying risks to your identified business assets and making an educated guess at what the likelihood that event will actually occur in a year and how often that event will occur again.

These have so far all been enterprise level standards that you control.

Acceptable Use

The Acceptable Use category defines company objectives for establishing specific standards on appropriate business use of the company information and telecommunications systems and equipment.

The acceptable use category is all about what our end users have control over. Certain usage activities such as Internet traffic, email usage, telecommunications, social computing, and software usage all play a part in The Security Trifecta (Figure 7).

A user has the choice to behave inappropriately while using the company's technology assets.

An employee does not have a choice in how complex their password is because you have established an unbending standard defined in your asset management activities. Do you see the distinction?

When misconduct occurs, you need employees to know how to report it and to do so without being concerned about management reprisal.

Vulnerability Assessment and Management

The Vulnerability Assessment and Management category defines the company objectives for establishing specific standards for the assessment and ongoing management of vulnerabilities.

When I refer to vulnerability assessment and management, I am talking about the actual task of assessing security risks and the actual management of those risks (Figure 8).

Security vulnerabilities continue to emerge on a regular basis and if we are not vigilant in the identification, remediation, and even compensation of those risks, we increase the risk to our enterprise not to mention the people who depend on our work whether they realize it or not.

Threat Assessment and Monitoring

The Threat Assessment and Monitoring category defines company objectives for establishing vigilant standards for the assessment and ongoing monitoring of threats to company information assets (Figure 9). The latest buzzword in the business is threat modeling which is really just a fancy term for placing a value on our business assets and making determinations about potential threats to that intellectual property or business asset.

Remember, security and governance are cost centers to the business, not profit centers, so the traditional return on investment ROI models do not work properly when making your case for funding. You need to speak to other business leaders, especially the ones approving your budget, in a business language. I've seen many formulas to calculate what we need to spend on security controls and the only one that makes sense to me and to the CFO is a simple thing called ALE or Annualized Loss Expectancy. This is something learned by MBA and accounting students alike. The very first thing you should be doing is placing a monetary value on that business asset you are charged with protecting. Other executives, such as the CFO, would be the best person for this information.

To provide hopefully a brief explanation of how it is calculated, there are two factors that comprise the ALE. They are the Single Loss Expectancy (SLE), which is the percentage of the asset you are attempting to protect that would be lost in a single exposure, and the *Annualized Rate of Occurrence* (ARO), which is the frequency the loss event occurs in a year. Those two factors multiplied together give you're the ALE (ALE = SLE * ARO) (Figure 10).

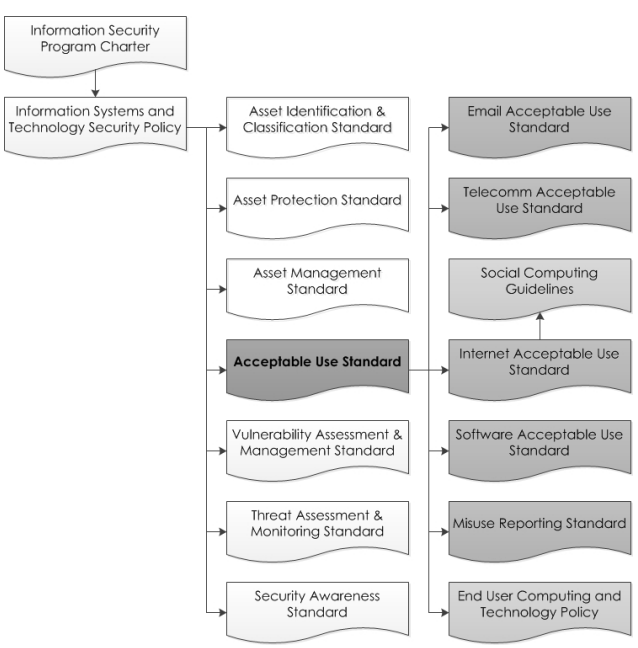


Figure 7. *Acceplable Use Standard*

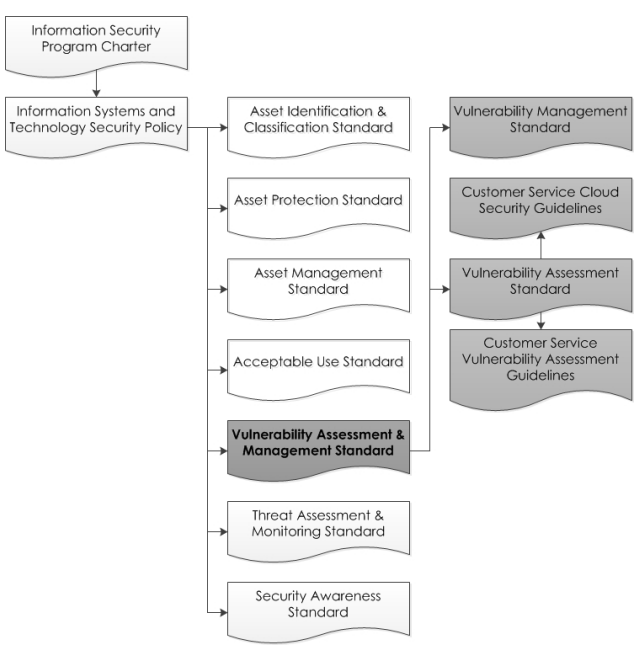


Figure 8. *Vulnerability Assessment & Management Standard*

For example, suppose than a business asset is valued at $200,000 and the single cost of exposure is $50,000. Your SLE is now defined as $50,000 right? How many times in a year do we expect this exposure event to occur in a year? If we expect an exposure to occur once every year, then ARO is 100% whereas if we think there is a 50/50 shot, our ARO is now 50% right?

Once you have these numbers, some simple math will enable you to make a stronger business case for security initiatives because you will be speaking the language of business and not technology which goes a long way in the board room.

Now that you have identified and placed a value on your business assets, you must monitor your controls effectiveness. In the realm of monitoring, consolidation and centralization of your command and control will help you master your domain.

Security Awareness

The Security Awareness category defines Company objectives for establishing a formal Security Awareness Program, and specific standards for the education and communication of the Information Security Program Charter and associated policies, standards, guidelines, and procedures (Figure 11).

The final task you have in the governance domain of The Security Trifecta is security awareness. When I talk about awareness, the essence is really about educating your users of the business technology and resources on the rules you have implemented.

Here is a question for you; do you have today a security awareness policy? Now, do you have third party relationships with vendors, auditors, or guests who in some way utilize your business technology or assets? Last question, does your security awareness campaign extend beyond the company's employees to these third parties? Chances are you have these third party relationships and you must be bringing awareness to these people about your expectations for their usage.

To put it another way, in my home, when someone visits me, they are required to remove their shoes before entering my home. I do this not to be a pain, but to keep the dirt and grime they have accumulated on their shoes outside from making my home dirty. I look at my IT security policies the same way. Why should I allow your computers viruses and other malware into my corporate house? If you have disk encryption, security software, and are properly patched, I'll let your computer join my

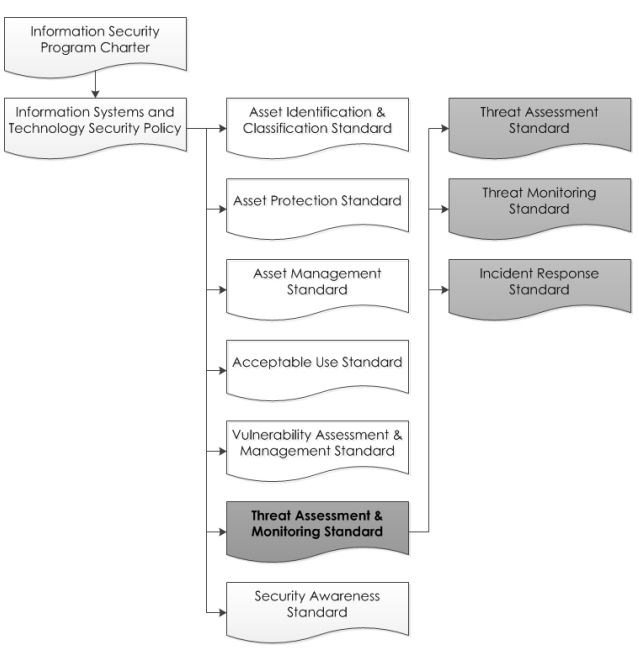


Figure 9. *Threat Assessment & Monitoring Standard*

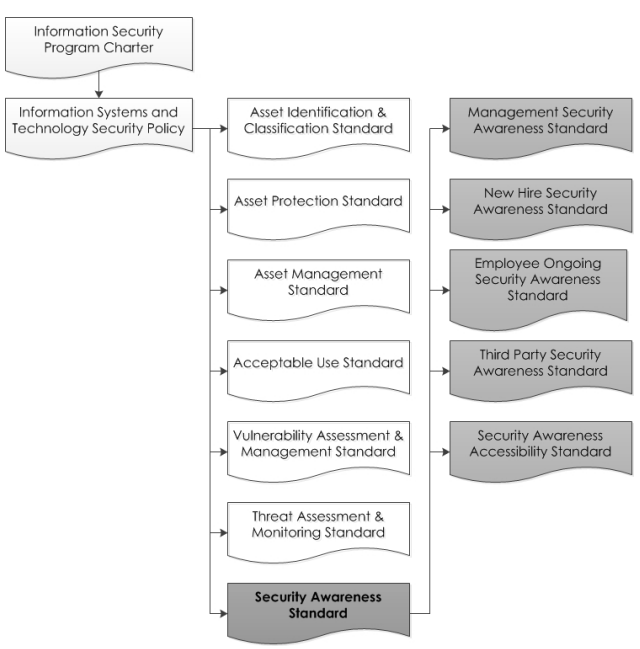


Figure 11. *Security Awarness Standard*

Figure 10. *Annualized Loss Expectancy Formula*

network. Make sure that your awareness campaigns include new hires, ongoing employee, and third party users.

Technological Application

Now that we have the foundation of our information security program built upon the governance framework we have constructed, what next? How do we enforce these rules effectively? With technology and technological controls that enforce our governance program of course!

Within the technological environments of any organization, some facets of technology are hard-coded and enforcement of those business rules is unbending. In other instances, employees or other individuals using those systems have a degree of latitude to make decisions on the usage of that particular technological permutation.

If you think that absolute security exists you would be absolutely incorrect. The reality is that security is a process of risk identification, mitigation and vigilance. It is incumbent upon both the security professional and the supporting leadership to first identify what must be protected in order of priority. Next we mitigate or otherwise offset the risks by using technological tools and procedural changes that are institutionalized. And finally, we apply vigilance to keep ahead of the threats that exist. Vigilance involves personal education in any form, be it formal or self-guided, and the discipline to carry through the charter we pledge to adhere to as security professionals. Security is a process; it is an integral part of our business. Just like any business process, security must be updated, tweaked and tuned. The consequences of not adhering to this philosophy are potentially catastrophic. Many organizations and security professionals are running on borrowed time. I'm not prophesying that there is no hope for security. Quite the contrary! What I am suggesting is that a healthy dose of reality be introduced into the mixture. We must understand that mitigating risks are more important than mitigating fear with a false sense of security.

The key is to implement governance standards that are holistic enough to establish the organizations command-and-control while remaining agile enough to adapt to the natural progression of technological permutations. You will want to avoid being too restrictive and too specific because this will introduce unnecessary loopholes which will be taken advantage of by employees and third party's alike.

You must find the point of technological equilibrium that balances the maximum level of information security without negatively impacting the core business processes that you are protecting. Security should not be a barrier to business, but an enabler to business.

Vigilance

Now that we have the governance structure instituted and the technological controls implemented to maintain our utopia, what is next? Are we at the place where we get to congratulate ourselves and take a long vacation? Sorry, as security leaders, I don't foresee a long vacation in your horizon which brings me to the *Vigilance* part of The Security Trifecta.

The reality is that nothing works very well without teamwork. Controls and standards break down without careful tending just like weeds take over our gardens without vigilance. We must regularly review our security standards validating their relevancy and we will remain agile to adapt to the changing business landscape putting into practice carefully considered revisions to our ongoing security program. We must always strive to be active, not reactive in our pursuit of information security excellence.

There is nothing perfect in this world that people have made or accomplished. That being said, it is incumbent upon us to monitor, test and improve our creations. Information is your friend and the more information you collect, the better understanding you will have of what you are protecting.

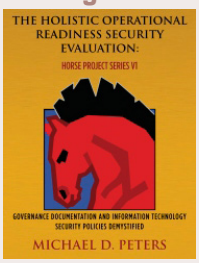
Now that we know a lot about out systems, it is a good time to help others understand how they affect them through awareness education activities. When we help others understand why we do the things we do and they see the relationship to how they do their work, most of them will begin to increase their support for you and your mission.

Conclusion

Being technologists, we all understand that we share the same common challenges that face every other company. Security threats are only tempered by putting into practice The Security Trifecta. This approach applies to everyone with few deviations. The foundation to our successful IT security programs are built with a holistic approach toward governance. Every facet of our governance program must be reviewed on a regular basis in order to maintain its relevancy to the organizations.

Security threats will never go away and the challenge bubble will only get bigger until we either proactively or reactively adapt to it. Our world is

Closing Comment



I've mentioned many IT security governance policies in this article. You may already have these ratified but in the event that you do not, a comprehensive suite of governance documents are available in my book *Governance Documentation and Information Technology Security Policies Demystified* which will put your organization on the fast track.

globally connected and increasingly interactive through technology. I challenge security and business leadership alike to join together at the same table and leverage each other's strengths for the collective good. No more myth propagation, no more corner cutting for the sake of expediency or marginal gain, no more discounting the importance of security to business and individuals alike.

Feel free to connect with me in our common professional networks. I'd welcome sharing ideas with you on increasing the effectiveness of IT security governance.

MICHAEL D. PETERS

Michael D. Peters has been an independent information security consultant, executive, researcher, author, and catalyst with many years of information technology and business leadership experience. He has been referred to as the "Michelangelo of Security". Michael's current and previous executive positions include Chief Security Officer, Chief Information Security Officer and advising Chief Information Officer. From a credential perspective, Michael holds an Executive Juris Doctor in Cyberspace Law; a certified MBA in IT Management, undergraduate degree in IT Security, CISSP, CRISC, CISM, CCE, CMBA, SCSA and he is an ISSA Hall of Fame recipient. In the realm of thought leadership, Michael is the author of "Securing the C Level", "Governance Documentation and Information Technology Security Policies Demystified", "The Security Trifecta" and thousands of blogging, tweeting, social media networking and professional network syndication and industry feature publications. He has contributed significantly towards curriculum development as adjunct professor for graduate degree information security, advanced technology, cyberspace law, and privacy programs and toward industry standard professional certifications.