Developing a Framework to Improve Critical Infrastructure Cybersecurity

Velocity Partners Security & Compliance

Doug Stoneman, **BA, CISSP, ISO/IEC, PII, MCP, IP**

Use of Frameworks, Standards, Guidelines, and Best Practices

1. What additional approaches already exist?

There are a number of frameworks available but the major frameworks that I very is that specifically deal with cybersecurity are: ISO, COSO, COBIT, NIST and ISF. For the most part businesses not involved in government contracts or infrastructure use as best practices ISO-27K, COBIT or NIST as their business frameworks. However it should be noted with a high degree of relevance that these same organizations rely mainly on technical means for cybersecurity and not upon any framework. This is where the gap exists between protection of the infrastructure and cyber security that security frameworks are not applied.

2. Which of these approaches apply across sectors?

The four major ones apply across all sectors and those are ISO, ISF, COBIT and NIST.

3. Which organizations use these approaches?

It is easy to determine which organizations are certified with ISO-27001 because they are certified and those companies that are certified are listed on the ISO site. However there are only 105 companies that are certified for ISO 27001 in the United States. The ISO certification requires that the leadership or executives of the organizations put forth a statement of compliance that they will enforce correct the framework. Also everything of the sector within the framework must have a risk assessment performed upon that sector and upon the controls or standards within any sector and those organizations must develop and maintain a risk treatment plan known as the RTP. Recertification must occur every three years with ISO-27001.

4. What, if any, are the limitations of using such approaches?

There are no continuing limitations to using any framework; the only limitations that would occur would be based on performance of those individuals' within the frameworks.

5. What, if any, modifications could make these approaches more useful?

Companies and organizations often modify frameworks to fit the needs of their companies and organizations so it is not unusual to make modifications with frameworks. However the major Gap is the implementation of frameworks, for example a framework that is not mandatory and has no authority from C level management or organizational leadership is not effective or efficient. Combining this non-mandatory approach for a framework combined with a sense of an organization that believes that technology is the only solution to cybersecurity is flawed. Organizations that maintain that they are "compliant" with this or that framework is suspect at best probably have a bunch of manuals sitting on a shelf collecting dust. Frameworks should be certified like ISO–27001 to ensure that they have the policies, standards, procedures in place to assure that they have a good cybersecurity plan. NIST should become a certifiable framework for information cybersecurity. NIST should be a certifying agency and test the policies and controls

of an organization that wished certified. NIST could also recertify so organizations could remain NIST certified instead of NIST compliant.

6. How do these approaches take into account sector-specific needs?
Frameworks are about business needs and building a mature business practice in sectors e.g. cybersecurity, asset protection and incident management for business needs within the mature business model. Risk assessment and management are business requirements as is the assessing of the costs of technologies. Each business need affects a sector and must be addressed by these business requirements within the business model and its practice.

7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?
Voluntary program(s) do not in the current cyber environment and neither do voluntary "guidelines" or "standards'. Most business frameworks or standards that have successfully implemented are mandatory in nature either by law, executive order or industry mandate. An excellent example is PCI and PII. PCI a financial standard for the payment card industry, if you want to play in that arena you have to be certified in PCI through and industry-standard. PII which is Personally Identifiable Information is about identifying and protecting the personal information of customers and clients, the PII standard is enforced by laws and government regulations and standardized requirements for contractors, military and presidential mandates. It is very expensive for companies to develop policies needed to enforce any sector of specific standards and build the controls that are derived from those policies. Implementation is also very expensive and time-consuming; it requires the employees of the organization to change what they are doing and in some cases is very specific. Faced with this change is it any wonder that implementing a new framework is difficult for organizations to do.

8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?
A good example of this is the international standards organization they play a very large role in sector specific agencies and related sector coordinating councils for ISO-27001. Along with new white papers on specific guidance for sectors and additional schedules for assessing specific areas coordinating council's very helpful providing guidance and directives for business units.

9. What other outreach efforts would be helpful?
Specifically for NIST explaining the difference between a mature business model and its advantages for the cybersecurity sector, explaining that technology alone is not the complete answer; that technology must be combined with the business model that is effective and efficient and has the flexibility and scalability to meet cyber security threats. An analysis of past cyber crime(s) in the cybersecurity sector has shown the technology offers limited protection and that the bottom line is that technology alone will not be enough to protect companies or organizations.

The hackers in the fraudsters are using ever more sophisticated techniques; malware has been reported inserted in some preproduction PCs and other hardware that consumers and companies buy. The race between security professionals and the Hacktivists infrastructure a.k.a. hackers, fraudsters, organized crime, and unfriendly governments, are engaged in a war of information; and much like the cold war it is move and counter move with collateral damages to the economies of nations.

In a landscape of breached security and defeated encryption the typical reactive technological security infrastructure response is that more technology is the answer to threats and that one more layer of security technology will solve the security issue. It is that very nature of the reactive security industry and the focus on technology that is the scale and scope of the problem. According to Price Waterhouse Cooper (PWC) cyber crime is a global crime and in 2012 PWC ranked it as one of the top four global crimes in the world and that one quarter of the organizations surveyed were victims of some sort of cyber crime. [1] However as with any Global contest, to win or at least counter, it must be fought with a strategic plan that has specific objectives and is organized, flexible and not reactive. Hacktivists technology is driven by innovation; incidents of hacking are "technology-driven innovation" and are entrepreneurial in nature it is a crime of opportunity. The hackers did not invent internet protocols, the Internet or even the code they use in hacking; they are opportunists, taking advantage of existing technology and using it in new ways, hence innovators and entrepreneurs (people who take risks). Companies and government agencies are reactive in nature, there are no strategic plans nor are there any specific goals that can be identified as to what comes next. The United States Federal government and Congress funded and anti-cyber division in 2010 to protect the information technology infrastructure of the United States. This division is known as the National Cyber Security Division (NCSD). The objectives stated on their website are to protect the cyber infrastructure and the goals listed on their website are to build and maintain an effective national cyberspace response system, and to implement a "cyber risk management program" for the protection of the critical infrastructure. These two objectives are very broad in scope and are of course reactionary e.g. a response system for what, responding to whom, what is the endgame? A "cyber risk management program" to protect the infrastructure, power plants, dams, transportation systems, interstate highways, and water systems, all of these are real systems they exist in the real world. How does one in effect create a "cyber-risk" management program" if one has no control over the business management systems that run them?
This is reactive in nature and the Goals are quite vague about the overall responsibilities, goals and objectives. The NCSD may indeed represent ongoing technical and tactical information to federal government agencies like the FBI, CIA, NSA, NTSB and others and may assist in investigations and information warehousing information about existing and current threats. However this is reactive in nature and is not a trending analysis about where the Hacktivists community is going, what their goals are, the kinds of tools will they will be using in this future. Who will be cooperating with them not to mention how to find and defeat them? An example of this is "The management Risk Program" in the public release at the Black hat security conference held the week of July 23, 2012. Reuters international published a story about web connected industrial controls stoke security fears. This article is about a Kansas agricultural concern, the owner left the wind power generation system connected to the Internet without any password protections despite warnings from the Canadian manufacturer endurance when power. The vulnerability left exposed industrial controls many of them in critical facilities wide-open. This example buttresses concerns that critical national infrastructure and the Western part of the country is more vulnerable to hacking attacks now than two years ago despite its status as a top cyber security priority for the White House. [2] This is an example of a "cyber-risk" management program" having no control over the business management systems that run them.

The latest research indicates that specific sites that are visited or used by prospective targets of opportunity are used as "stepping stones" to conduct attacks against these targets. This intelligence reported by RSA shows complex planning on the part of the hackers choosing a

compound “man in the middle” or a “false flag” type of attack to gain Intel and information using a web-site trusted as harmless to inject malware. [3] Internet content provider Google detects 9500 malicious web-sites daily. [4] When one considers that most of these websites are unaware that their company web-sites own unwitting employees have been compromised, it is obvious that this type of attack will expand in the future. Recently (2012) new research from Forrester has reported that an estimated 80% of the owners of these websites are not aware of the compromise until an outside party notifies them; [5] furthermore this same research indicated that this injected malware site lasts a very short time. A study by the Anti-Phishing Working Group (APWG) found that “40% of cases phishing pages are removed from sites within 24 hours after they were planted and close to 60% of the respondents claim to have taken down the malicious websites within 2 to 3 days.” [6]

This type of complex planning demonstrates an overall flexibility on the part of the hackers and very fast timeline of the hack taking advantage of opportunities available on website's lack of monitoring, for hackers this represents a target rich environment. These tactics represent an issue for a non-technological response for security; it demonstrates that policies and procedures for monitoring the technology that is used for security are not in place or not complied with; when policies and procedures are not followed bad things can happen whether it is a company, industries or governments.

The hackers in the fraudsters are using ever more sophisticated techniques; malware is becoming more sophisticated and attacks are more strategic in nature and less random. Google and the international Computer Science Institute warned that the so-called drive-by downloads are becoming the attack of choice. Of the 77,000 malicious URLs Google identified carrying malicious payloads, it found that there were two toolkits used, “Blackhole” and “Incognito”. [7]

It is very important that policies and procedures be developed to meet this complex and strategic formulation of attack, not having strong policies and valid procedures that are derived from those policies makes any organization vulnerable to these types of attack. Not having strong policies and good procedures in a good security practice can produce some extreme results. It is clear that the attackers are now using automated malware as a complex methodology in their attack scenarios. This means that the augmentations and changes in the attack no longer have any human operating it is created by an automated program much like any other automated program that you might use for say document publishing database searching or any logical query or all logarithmic substantive programming. AV technology is signature-based, this is of course reactive, a signature once found in the wild piece of malware running is identified a signature of that malware is constructed and it is put into an update in the AV technology. This reactive type of antivirus is insufficient and outpaced by automated malware technology, so blocking in eradicating that malware is now not possible. A good example is the "zero – day" malware which is being constantly changed and updated there can be no signature to this type of attack; rather a behavioral analysis must be performed to identify the vectors of the attack and the attacking malware. It now becomes imperative that looking at what the malware is doing or has done to identify at rather than what it looks like. [8]

It now becomes imperative that policies and the derived procedures must be in place for the IT security professionals watching for the possible or probable attack, behavioral type procedures can be put in place to identify these kinds of attacks, and this type of constant monitoring is not reactive it is proactive. If a company does not have policies or procedures or those policies and procedures are not followed bad things can happen.

There are indeed many examples of this there is not time or space in this article to list them all, so a few examples of the nature of this concept will be examined. Two of the examples are from industry and one is from government, intelligence specifically, the government example is a procedural error from policy where people died. This is not to say that when one does not follow policies and procedures in the company people will die it is to underline the serious nature of what can happen when policies and procedures or both are not followed. However in government specifically in the intelligencer arena if you ask any intelligence officer from a local police department or to the CIA they will tell you if they make a mistake people could die. In industry it's rare that people died from a mistake of not following policies and procedures however the costs are very high, $3.7 million per incident or breach in the net diligence study October 2012; [9] The link to the study is in the reference number 10.[10] The breach caused per incidence of $3.7 million is an 18% increase from 2011 which further confirms the data that explains why number of breaches is dropping but the cost of breaches are rising. There is only one explanation and that is that the attacks are more concentrated more complex and automated and that strategically the number of the attacks will drop the costs an**d** success of these attacks will rise.

These accounts are just a few of the documented attacks and weaknesses of our technology based protections. With increased attacks the cybersecurity sectors under pressure and rising costs technology will not protect you for you are up against a committed opponent was willing to adjust their tax with technology so technology as a defense is not effective. What is effective is a framework that applies a mature business model to the cybersecurity sector it applies policies, standards and procedures that must be followed. There are plenty of models for this that may build a mature business model and provide flexibility, efficiency and scalability for a business model for risk management. There is a meta-framework which defines, simplifies, protects, monitor, report and at the center is your repeatable reliability. There is SIX Sigma's DMAIC which is: designed, measure, analyze, improve, control cycle, this was later expanded to RDMAICI are: recognize, define, measure, analyze, improve, control, standardize and integrate. The ISO 27001 model which is basically the same idea as RDMAICI only ISOs model is shortened to PDCA which is: plan, do, check and act. The scope of COBIT is based on the seven criteria which are: effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability.

All of these standards and frameworks purport to effectively do the same thing and cover some of the same controls for the most part. Any program that involves any kind of mandatory controls should be flexible enough to allow the company or organization's to select the framework that fits their business model there are many frameworks out there to select from and hence should not represent a significant issue. It is clear that technology is not enough to provide security and to protect the United States infrastructure. In terms of cybersecurity the technology is not the complete answer however a mature business model that mature business model combined with technology is very important for a cybersecurity framework.

Citation Box

[1] Info security magazine, December 01, 2011, One quarter of firms hit by cyber crime, survey says. Source: http://www.infosecurity-magazine.com/view/22389/onequarter-of-firms-hit-by-cybercrime-survey-finds/34

[2] Reuters – (International) July 23, 2012, Web-connected industrial controls stoke security fears, Source: http:/www.reuters.com/article/2012/07/23/us-blackhat-industrialcontrols-idUSBRE86M14R20120723

[3] Krebs on Security – (Int)September 25, 2012 Espionage hackers target 'watering hole' sites. Source:http://krebsonsecurity.com/2012/09/espionage-hackers-target-watering-holesites/

[4] Ars Technica – (International) June 19,2012 Google bots detect 9,500 new malicious websites every day. Source http://arstechnica.com/security/2012/06/google-detects-9500-new-malicious-websites-daily/

[5] Infosecurity – (International) September 24, 2012, Most data breaches come From within. Source: http://www.infosecurity-magazine.com/view/28404/most-data-breaches-comefrom-within/

[6] Softpedia – (International) September 19, 2012, Victims of phishing attacks unaware their websites are compromised, APWG finds. Source: ttp://news.softpedia.com/news/Victims-of-Phishing-Attacks-Unaware-Their-Websites-Are-Compromised-APWG-Finds-293391.shtml

[7] V3.co.uk – (International) October 2, 2012, Blackhole responsible for a third of drive-by download attacks. Source: http://www.v3.co.uk/v3-uk/the-frontline-log/2214082/blackhole-responsiblefor-a-third-of-driveby-download-attacks

[8] October 15, 2012, Wilson, Tim, Dark Reading – (International) Next-generation malware: Changing the game in security's operations center. Source: http://www.darkreading.com/security-monitoring/167901086/security/security- management/240009058/next-generation-malware-changing-the-game-in-security-s- operations-center.html

[9] Tsikoudakis, Mike October 9, Business Insurance – (International) Average insurance cost per data breach rises to $3.7M: Study. http://www.businessinsurance.com/article/20121009/NEWS07/121009907

[10] Greisiger, Mark, NetDiligence® , "October 2012, Cyber Liability & Data Breach Insurance C's laims, "A Study of Actual Payouts for Covered Data Breaches", Source: http://www.netdiligence.com/files/CyberClaimsStudy-2012sh.pdf

Specific Industry Practices

In addition to the approaches above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry.

NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

- Separation of business from operational systems;
- Use of encryption and key management;
- Identification and authorization of users accessing systems;
- Asset identification and management;
- Monitoring and incident detection tools and capabilities;
- Incident handling policies and procedures;
- Mission/system resiliency practices;
- Security engineering practices;
- Privacy and civil liberties protection.

Overall there is a general separation of business operations and IT operations this separation is due to the belief that technology is the only answer to cybersecurity. That IT cybersecurity is a cost center and thereby are assigned as a non-business sector. Companies seem to fall into a separation of sectors of security and IT. If a survey was done with asking organizations; "*Is there a line between your information technology department and your information security department?*" I estimate more than 75% of the time the answer would be yes. Companies and organizations do a relatively good job of encryption key management however most companies use a 128 bit key bit encryption. Most experts in the field state that a 128 bit encryption key is not sufficient given the threats that are currently out in the cybersecurity area.

Identification and authorization of users, accessing systems, asset management, incident detection and tools and incident handling procedures are sectors where most companies fail. It is common to find companies with sectors of identification and authorization to find users that are dead, gone for years, ex-contractors all still active in their systems with many cloned users in their active directory tree. Most companies have some kind of incident management plan but the plan is unrealistically simple, they believe they will not be a victim in an incident.

I would call system resiliency with companies and organizations a random sector, in most of the companies I've worked with I have found points of single failure. When these single points of failure were identified it was often met with a "we will deal with that later" attitude, of course that single point of failure almost always occurs. Then the company or organization spends a magnitude more money fixing the problem than the original cost of mitigation when the single point of failure was identified.

As stated before security is often separated as a business unit from the information technology business unit, there seems to be resentment between the administrators and managers of IT departments against managers of security departments. This is a legacy from the 90s were systems engineers and administrators and IT personnel could do pretty much whatever they wanted when they wanted but it has no place in the current cybersecurity sector and serves no useful purpose. The alternative is that the company or organization is using a divide and conquer strategy for the cybersecurity and IT business units to pit them against one another for any number of reasons. Those reasons would be to reduce costs, to deflect responsibility away from management when failures and breaches occur to blame the IT and/or the cybersecurity sector. With the advanced of frameworks it is quite possible that the failure to fully implement a security framework can be blamed on the performance or lack there of from the IT and security departments. For whatever reasons one chooses there is a divide between the information

technology departments and the security departments and it makes using a framework to enhance cybersecurity impossible.

Security policies are written and not followed as they are not approved and supported by top level management. Implementation of a security policy that is not approved by top level management is an exercise in futility. The supported and approved security plan by senior management has the purpose of finding out how things really work and provides actual metrics for senior management. It is interesting that there are a host of companies out there that seem to believe that if they have a plan, a piece of paper on the shelf, that this will actually suffice as some kind of protection for them, it is nothing more than wishful thinking. It is a huge false assumption and a large assumption of risk on the company's part and provides no protection for the business sectors and certainly no due diligence. Only an established framework with a mature business model will aid with the technology both in terms of operation, metrics and scalability. A mature business model like those provided by a framework will yield an accurate assessment of risk, asset identification, incident handling policies and procedures, system resiliency's, scalability and metrics by providing a mature business model inside of IT.
Security whether it is physical or cybersecurity is a process it is not a technology. I would recommend that NIST through NICE should have as a priority for the education of companies and organizations that **cybersecurity is not a technology it is a process and processes to be effective need a business model, a framework**. Lack of documentation, not checking logs, poor planning and bad management all contribute to a fundamental failure of information security. There is a very old saying and it goes; “People do not plan to fail, they just fail to plan." Failure as a function of process is expensive.
Information security and/or cybersecurity are about the business processes in place including all policies standards, procedures. The ability to apply knowledge and experience, to capture new knowledge and learn from your mistakes is a definition of flexibility and scalability.
It is about business processes not about technology.

Velocity Partners
Doug Stoneman, **BA, CISSP, ISO/IEC, PII, MCP, IP**
262-790-0800 - office
414-708-2914- cell

Providing high quality IT support and services to customers since 2000