InfoSec Technology Management of User Space and Services Through Security Threat Gateways

Abstract

The focus of this paper will demonstrate the need to clearly define and segregate various user space environments in the enterprise network infrastructure with controls ranging from administrative to technical and still provide the various services needed to facilitate the work space environment and administrative requirements of an enterprise system. Standards assumed are industry practices and associated regulatory requirements with implementations as they apply to the various contextual applications. This is a high level approach to understanding the significance and application of an effective secure network infrastructure. The focus is on end user needs and the associated services to support those needs. Conceptually user space is a virtual area allocated to the end user needs identified with specific services to support those needs by creating a virtual playground. To manage risk, the concept of creating a "security threat gateway (STG)" isolates and secures each user space with its associated services. Emphasis will be placed on the functional managerial process and application of the STG, safeguarding one user space from another, to facilitate the use of the needed services to perform the operational tasks of the organization. When user's needs and associated components are clearly identified, then it is possible for anyone to use this model as a template, to guide them in creating an effective strategy for their own network security. This approach is practical in orientation and application, focusing on a high level perspective and assumes the reader already has a low level technical background for a tactical implementation in mitigating risk to the enterprise network infrastructure.

General Terms

Management, Measurement, Documentation, Performance, Design, Security, Human Factors, Theory, Legal Aspects.

Keywords

Security Threat Gateway (STG), user space, user services, DMZ, virtual playground, regulatory compliance.

1. Introduction

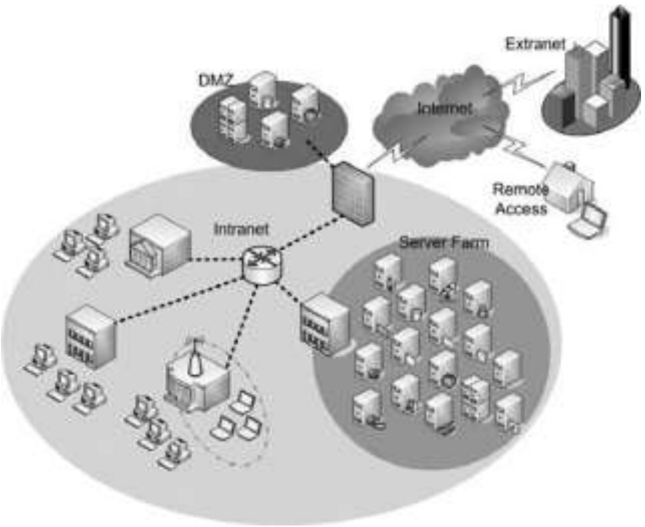
Within the confines of an enterprise network infrastructure, it is easy to mismanage resources and allocate levels of trust inappropriately. Extremes range; from being open and liberally allowing access to any and all resources and services, to being closed and disabling access and desperately needed functionality to legitimate users. The Internet hacker's social mindset, orientation, and strategy of for attacks have remained basically the same [21]. Current trends for Information Technology security exploits have progressively placed more emphasis on targeting common network services and exploiting vulnerabilities from trusted "insider" connectivity by various methods; ranging from social engineering, to exploitation of network services, as related to the hardware and software [18]. The challenge any information technology manager faces is to balance to the needs of both trusted and non-trusted users as they operate within the confines of the enterprise network infrastructure. The objective of this writing is to clearly present an alternative process and perspective that can assist any organization in their risk management methodology as it applies to securing the enterprise network infrastructure and facilitating the user's operational service needs.

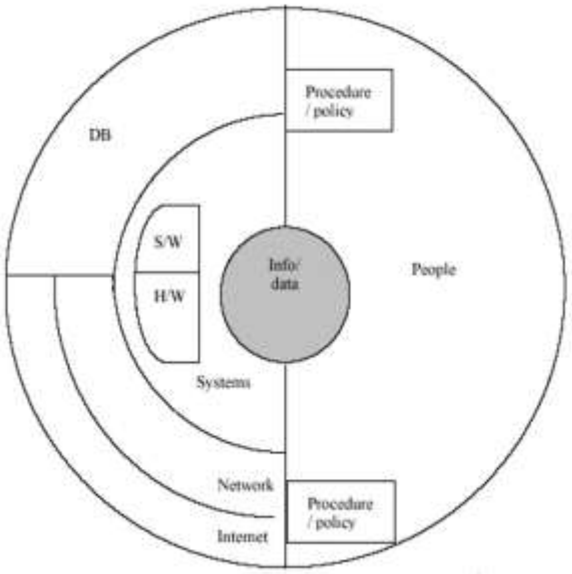
2. Techniques and current management practices

One of the more common techniques for securing the network infrastructure is a linear approach, in which virtual network topography is identified for access to the various services that are available (see Figure 1). These services are isolated by physical boundaries (separate physical layer networks), virtual filters (Access Control List's, Virtual Local Area Network's, firewalls, etc.), and administrative controls (policies, procedures, standards, and guidelines). These boundaries are typically referenced and generalized as the Intranet, Extranet, Internet, and DMZ. This concept can be further illustrated by a ripple effect of rings, extending from the data or service being protected (see Figure 2), out to the authorized source attempting to access the data from various geographical / logically referenced locations, with each ring representing a control being implemented to protect the confidentiality and integrity, ensuring only authorized access is granted. The key point of this illustration is that the network infrastructure is static and not based upon user needs, but instead on geographical access and proximity to the resources.

Figure 1. Typical Network Infrastructure Paradigm

Figure 2. Scope of Security Influence [1]





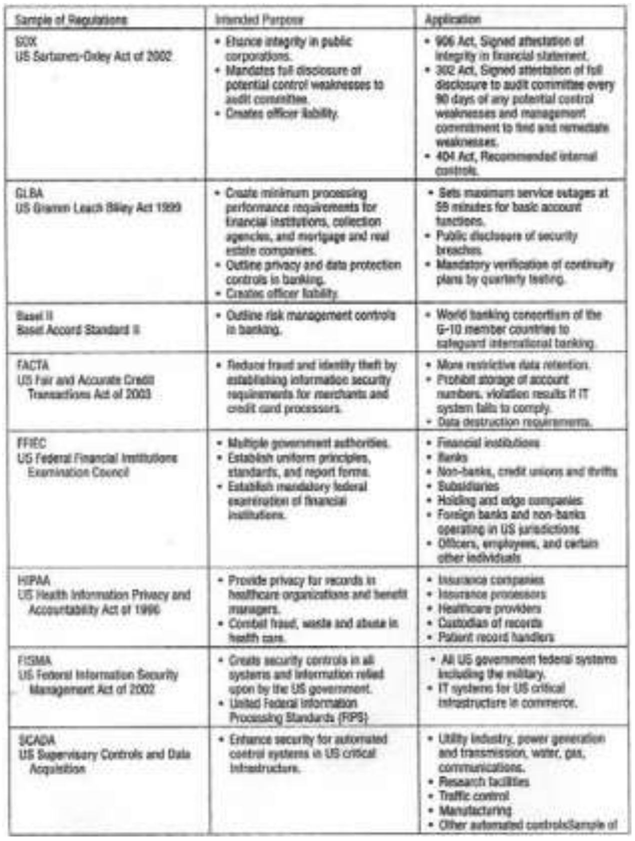
There is little flexibility and security in this approach, since users with various levels of trust are capable of physically moving from various geographical boundaries that may afford them access. If other, more sophisticated security implementations are not put in place to safeguard the organizations assets, loss or compromise of resource is inevitable. The users' geographical movement is what the hacker hopes for, so the machine that was compromised on the outside can inadvertently be moved inside, closer to more valuable resources for exploitation [13]. So, even though users' access may be limited through some authentication, authorization, or accounting methodology (Active Directory, LDAP, NDS, RADIUS, TACACS, etc.), the compromised system is still located behind most of the basic security intervention systems tactically designed to mitigate risk. A common example of this is seen in the worker who takes their work home on the company laptop and hooks up to his or her own Internet connection, where it is attacked, and compromised. The worker unaware that his or her system has been compromised later brings the same device back into the work environment. Now, the hacker has a compromised device sitting in the inner confines of the organization, able to bypass many of the security implementations set up to mitigate risk. A better model would to create a system that was not location specific, and flexible enough to accommodate the user depending upon their work or service requirements [20].

It is very common to reference services and resources in these general terms, and even more common to lockdown individual's understanding in how networks should function through the boundaries and limitations they create. Simply, these concepts though created to help structure our understanding have become obstacles in providing the services, resources, and security that is needed to effectively manage the modern network infrastructure. Information technology must assist the organization in meeting their objectives, while at the same time not introduce additional risk that could threaten its viability. Many organizations have been challenged with the pitfalls of the traditional enterprise network infrastructure paradigm, and have joined forces to combat the rising tide of hacker infiltration [6, 8].

3. Recognition of the challenges for network infrastructure security

Information Technology Risk Management has challenged the world and many organizations have been forced to embrace rigorous safeguards in order to continue exchanging in the market place. There are many published standards that provide basic templates of consideration for managing an information technology framework to address risk. One such standard is the COBIT from the Information Systems Audit and Control Association (ISACA); in which managerial, operational, and technical controls are all given consideration so an organization can be effective. The same threat does not exist for each organization, though there may be complementation between types of organizations. So each organizational entity must evaluate their information technology processes to determine which threats exist, and what regulatory compliance requirements apply to those processes [9]. A financial institution does not have the same information technology processing responsibilities as a hospital [5]. Though, if you were to compare, a large university or college institution that also had a medical school, to either a financial institution or medical facility, you would clearly see an overlap and complementation of regulatory compliance requirements [7]. Table 1 highlight some of the various regulatory characteristics required that every organization must consider in their information technology implementation. The significance of including this reference, along with user operational considerations; is risk management requires a thorough working knowledge of the of the information technology processes as it relates to the content, use, and accessibility of the data being maintained [17]. The significance here is that not every organization handles data that would need consideration under the United States Health Information Privacy and Accountability Act (HIPAA), but they instead may need to consider some of their financial transactions as they apply to the United States Financial Institution Exam Counsel (FFIEC) constraints [2]. Every organization, without exception, must have a data classification process in place that clearly identifies the roles of the data owner, user, and custodian with their associated responsibilities and access considerations.

Table 1. Sample of Common Regulations and Best Practices [2].



Sample of Regulations	Intended Purpose	Application
SOX US Sarbanes-Oxley Act of 2002	• Ehance integrity in public corporations. • Mandates full disclosure of potential control weaknesses to audit committee. • Creates officer liability.	• 906 Act, Signed attestation of integrity in financial statement. • 302 Act, Signed attestation of full disclosure to audit committee every 90 days of any potential control weaknesses and management commitment to find and remediate weaknesses. • 404 Act, Recommended internal controls.
GLBA US Gramm Leach Bliley Act 1999	• Create minimum processing performance requirements for financial institutions, collection agencies, and mortgage and real estate companies. • Outline privacy and data protection controls in banking. • Creates officer liability.	• Sets maximum service outages at 59 minutes for basic account functions. • Public disclosure of security breaches. • Mandatory verification of continuity plans by quarterly testing.
Basel II Basel Accord Standard II	• Outline risk management controls in banking.	• World banking consortium of the G-10 member countries to safeguard international banking.
FACTA US Fair and Accurate Credit Transactions Act of 2003	• Reduce fraud and identity theft by establishing information security requirements for merchants and credit card processors.	• More restrictive data retention. • Prohibit storage of account numbers, violation results if IT system fails to comply. • Data destruction requirements.
FFIEC US Federal Financial Institutions Examination Council	• Multiple government authorities. • Establish uniform principles, standards, and report forms. • Establish mandatory federal examination of financial institutions.	• Financial institutions • Banks • Non-banks, credit unions and thrifts • Subsidiaries • Holding and edge companies • Foreign banks and non-banks operating in US jurisdictions • Officers, employees, and certain other individuals
HIPAA US Health Information Privacy and Accountability Act of 1996	• Provide privacy for records in healthcare organizations and benefit managers. • Combat fraud, waste and abuse in health care.	• Insurance companies • Insurance processors • Healthcare providers • Custodian of records • Patient record handlers
FISMA US Federal Information Security Management Act of 2002	• Create security controls in all systems and information relied upon by the US government. • United Federal Information Processing Standards (FIPS)	• All US government federal systems including the military. • IT systems for US critical infrastructure in commerce.
SCADA US Supervisory Controls and Data Acquisition	• Enhance security for automated control systems in US critical infrastructure.	• Utility industry, power generation and transmission, water, gas, communications. • Research facilities • Traffic control • Manufacturing • Other automated controlsSample of

Technical considerations and approaches for a risk controlled environment have included adding various physical and logical mechanisms [15], to thwart or deter the hacker's capability to exploit the network infrastructure resources. The approaches for these techniques have been to passively defend, as well as to aggressively attack, or counter the maligning influence. Examples of these enterprise infrastructure architect modifications include: the Honeypot or Honeynet; network Blackholes, and visualization monitoring techniques. The basic tenant behind each of these approaches is to isolate the offending influence and control the level of impact they can possibly produce. Honeypots and Honeynets create enticing opportunities to draw the attacker to a specific monitored resource so that their activity can be evaluated, tracked and possibly prosecuted [16]. Blackholes have a different application, here the network infrastructure traffic flows are established to redirect offending traffic to nonexistent resources in an effort control the impact of malicious traffic and leave the hacker with a sense of confusion from the ubiquity they discover and explore [4]. Visualization tools and techniques, of various commercial and non-commercial applications display diagrams of real-time traffic patterns. The advantage to this approach, is that the human sensorial intervention can more quickly respond to perceived anomalies than can artificial intelligence from an appliance or software based IDS' s or IPS's systems [12]. Regardless of the approach, the intent is to mitigate risk by controlling the level of impact an offending influence can exercise within the confines of the enterprise network infrastructure.

The current effectiveness of the enterprise network infrastructure has been challenged in many ways. We briefly looked at the fallacies surrounding the traditional topographical layout and seen that the user's location and their ability to move fluidly across predetermined boundaries has introduced risk, regardless of the level of trust presuppose of the user. We have seen how, because of abuse, regulatory constraints have been introduced and a greater responsibility and liability for negligence has been imposed upon institutional use of data. Because of this regulatory compliance and liability, the use of data must be clearly defined, and responsibility identified down to the user level. We have seen that more technical consideration is being researched, for control over the level of influence an intruder can introduce to the network infrastructure and environment, and for development of appliances and applications that incorporate human sensory intervention to more quickly respond to an incident. All of these snapshots are organizational processes managing information technology threat identification and associated risk, moving beyond the scope of the traditional network infrastructure topological boundaries. The bottom-line is; what information technology is really being protected, and how effectively are we protecting it.

4. Discussion

Solutions for security of the network infrastructure and avoidance of hackers exploits have not really changed. Now it requires more diligence and caution in safeguarding a solution for the enterprise network environment. Consistent methods of highlighting awareness of vulnerabilities, and then of addressing the problem to the proper authorities or corporate stakeholders to determine a cost effective method to mitigate risk still applies. As with all approaches, emphasis should be given to reevaluating the vision and mission statement as it relates to the information technology process being implemented to ensure it does not detract or include unnecessary risk. This process should be systematic and depending upon the organizational objectives and meet the regulatory compliance requirements per Federal, State, or Industry standards. Typically regulatory constraints or guidelines address the problem and may present a model or standard for suggested implementation, but their primary focus is on the consequence of failing to properly manage the risk and the liability an organization will incur [10].

4.1 User profile characteristics and service needs identification process

As a good manager desiring to facilitate two-way communication, it is best to poll your users (or organizational groups), with a brief survey so that they can identify what the information technology needs exist to support their work processes. Depending upon your organization's intellectual makeup, the survey can range from very simple to very technical and complex. The significance regarding this approach is, everyone gets an opportunity to express their needs, and you the manager can then synthesize the results into logical groupings. This opportunity to contribute forces the user to negotiate through their operational requirements and heightens their awareness of the vision and mission of the organization, as well as the need to safeguard its assets and supporting resources [14].

Some of the questions to pose in the survey may look like this:

1 What information technology services do you need to perform your duties? Please briefly describe how you use technology on a daily basis.
2 Do you use email and if so do you require that it be sent securely, so no one but the intended user can read it? If so please describe a practical example in the past where this was necessary or would have been beneficial.
3 Do you use or exchange data that may be considered sensitive, and if so briefly describe how you do this?
4 Do you need information technology when you travel, or do you work from home? If so, what resources do you need access to, and for what purpose?
5 How long have you been with the organization and what is your current position?
6 How often do you use some type information technology, and what level of knowledge or experience would you classify yourself as, e.g., novice, intermediate, expert, or somewhere in between?
7 Does you department have any special needs or requirements that may introduce a threat to the overall information technology services on our network?

Through this polling and exchange procedure, we gain a greater familiarity with the individuals actually performing the operational needs of the organization. There many other questions that could and should be asked, but from this short set of questions and the feedback received, you can quickly start to identify possible threats and strategize a response to make their information technology experience beneficial without compromising security to organizational assets. This information can then be used to access the information technology in place, as well as the current controls, to determine whether information technology is supporting the vision and mission of the organization. One of the most common complaints about IT staff is that people can't perform the tasks required, with the support services and resources they receive. This needs survey process, provides valuable strategic information regarding the required services and the level of operational trust that can be afforded. This survey also provides the individuals being supported with information technology, a sense that their needs are being recognized, and there is a process in place to support those needs. A similar form of this survey could be completed periodically, so that as the vision, mission, or operational needs change, a tool is in place to reassess and justify the needs as they relate to the level risk that must be managed.

From this survey approach, groupings can then be created per the needs identified, providing a logical schema of user space, service space [20], and general overview of data that is being accessed (see Table 2 and Figure 3). For example, user one needs wireless access in an environment that poses a high risk [3] with basic internet access and Email, while the other users' spaces (two and three), have similar needs and require a greater level of trust and service need, but no wireless. It would be ineffective to limit everyone to the lowest common denominator of need with the least amount of risk. Instead, we must strategize, and redefine our enterprise network infrastructure paradigm to not be functionally tied down to the geography, but to be accommodating to the common services that groups of users need, while safeguarding their interaction within the enterprise environment.

Data Type	**Services**	**User One – Green (trusted – low risk)**	**User Two – Yellow (non-trusted – Medium risk)**	**User Three – Red (non-trusted – high risk)**
Public	HTTP	X	X	X
Private	HTTPS	X	X	X
General	NTTP		X	X
Public	JAVA		X	X
Public	ACTIVEX		X	X
General	VOIP	X		
General	VIDEO	X		
General	DHCP	X	X	X
General	DNS	X	X	X
Private	FTP	X	X	
Private	Database	X		
Sensitive	Imagining	X		
Private	VNC	X		
Public	Wireless			X
Public	SMTP	X	X	X
Public	IMAP	X	X	X
Private	File Shares	X		
Public	IRC			X
Private	VPN	X		

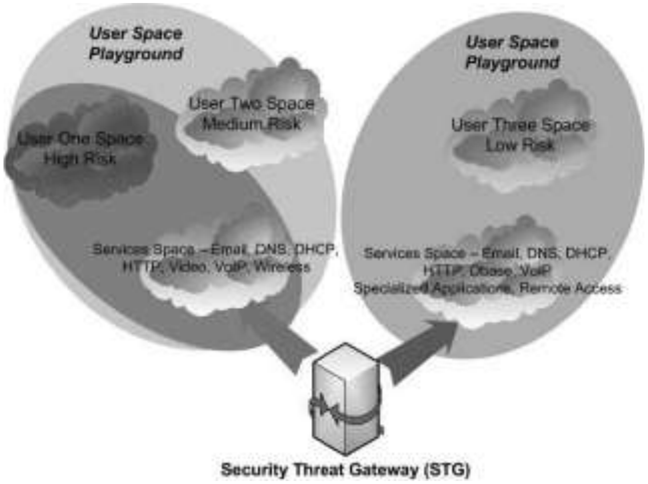

User Space Playground
User Two Space Medium Risk
User One Space High Risk
Services Space – Email, DNS, DHCP, HTTP, Video, VoIP, Wireless
User Space Playground
User Three Space Low Risk
Services Space – Email, DNS, DHCP, HTTP, Dbase, VoIP Specialized Applications, Remote Access
Security Threat Gateway (STG)

Table 2. User Space Service Needs Assessment Matrix

Figure 3. Logical Layout of User Space, Services, and Integrated Security Threat Gateways

An illustration of this concept is a “virtual playground.” The playground concept is where people with like interest and activities gather together to play or perform their duties. We see this everyday from children playing in literal playgrounds or adults enjoying their daily routine at the gym. The concept is no different. The significance is that the individuals can move from one location to another without affecting the vulnerability of the network because the proximity and use of the resources is governed and controlled regardless of location. The same concept can be applied to placing environmental controls around hazardous material so that its capability to corrupt is not allowed outside the boundaries of legitimate use.

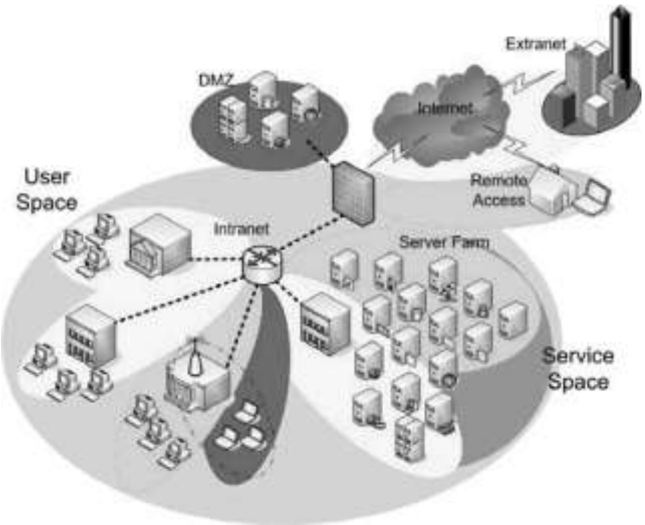


Figure 4. New Network Infrastructure Paradigm based on User Space and Service Space Needs

To ensure user’s space and the associated service space support their needs, various controls must be implemented to segregate one playground activity from another (see Figure 2). These series of controls for administrating security, is what I would like to suggest be referenced as a Security Threat Gateway (STG). A STG is a culmination of controls that include all the previously mentioned physical, logical, and administrative constraints. Where if you have a user space (see User Three, Table 1, Figure 3 and 4) that requires wireless as their primary means of network connectivity with services ranging from basic Internet to email, you definitely want to make sure they did not open up backdoors via a dual-honed connection once they come into your organization and connected up the Ethernet port. Here, Johnny or Jill Hacker, assuming the laptop was compromised, could easily backdoor your infrastructure at any point and time. Instead, we would want to identify this devices connection’s capability, the user space, and service space and provide a virtual environment where they can effectively perform their responsibilities. The playground solution is to either limit this device to specific VLAN’s via an 802.1x application, pushing this device’s request to services designated in the DMZ, or refuse connectivity altogether for the Ethernet connection. Here oblivious to the user, controls applied were both physical and logical constraints to manage and mitigate risk through technical controls. Further administrative constraints could be applied to give emphasis to the operational limitations for the “how and where” the device will be used with in the context of the enterprise network environment [19]. Additional consideration and administrative controls will need to be implemented for regulatory compliance per the type of data and how the transactions are being processed. A common example of this can be seen in how credit card transactions are processed and whether or not they align with the Payment Card Industry (PCI) Data Security Standard (DSS) constraints mandated by the industry.

Another consideration seen is, how some groups’ user space and service space may overlap or be a subset of another group. Here the decision making process of risk management is exercised to determine whether separate virtual playgrounds should be created, or if they should share the same user and service space. What is significant though is that this decision process is not arbitrary, or limited to the old topology paradigm of Intranet, Extranet, Internet, or DMZ; instead customization is facilitated for access to the resources and services the user needs to perform their responsibilities.

4.2 Tactical significance of the Security Threat Gateway in mitigating risk

With the rise of automated threats of Botnets and Puppetnets infiltrating enterprise network environments [11], it is imperative that the network infrastructure is no longer looked at as having a front and back door for access into the secure Intranet environment. The key benefits of the STG’s are that they create virtual choke points, and allow the system administrators flexibility in controlling how access to the various network resources are made available to users, allowing granularity to the type of service being offered. Now, many different virtual playgrounds can be created, with each having an associated, graduated level of risk, and key security assets devoted to monitoring the activity that passes through those choke points; e.g., intrusion detection and prevention devices evaluating irregularities and content filtering accessing data classification requirements. Figure 4, demonstrates both the virtual playground space and the STG which segregates each play area. This example is obviously over simplified, yet it illustrates that the level of support for the organizational operational needs, which are not limited to any predetermined geographical boundaries. Clearly, the internal wireless connectivity is regulated by the same level of trust and resources as someone who may be connecting from the Internet. Conversely someone connecting from home via a VPN connection is afforded the same privileges of services and resources access as if they were sitting at their work place system. Because the virtual playgrounds have been clearly defined and the STG’s put in place to manage all exchange between the services and resources, risk is mitigated, and customized support afforded to the end user needs to facilitate the organization’s operational objectives.

5. Conclusion and future work

Clearly limiting a risk management strategy to the traditional enterprise network topology will cripple either the effectiveness of the organization, or allow a level of risk that is difficult to manage and assess. The solution is to change our vantage point of the problem and redefine the network topology in terms of the operational needs of the user, and the associated services and resources. Once a thorough analysis and understanding is obtained, then both logical and physical structural constraints can be imposed to support the organizations’ needs, and mitigate risk. The methodology presented is a high level, simplistic process, which is intended to challenge the reader to look at the ways they are currently supporting the information technology operational needs, and consider an alternate method that can easily be assimilated into their current infrastructure. This method encourages and embraces operational user input for a corporately recognized solution to on-going challenges. This process alone will increase security awareness, and motivate individuals to be more sensitive in how they utilize their information technology resources.

The Security Threat Gateway is not a new concept as much as a redefining the functional application of that which is currently practiced in many network environments. This concept will hopefully challenge both the end user and system administrators to think beyond the mental boundaries that have imposed unnecessary limitations, as well as bring insight to applying greater levels of security to the practices and controls already being effectively implemented in their enterprise network environments.

6. References

[1] Amer, S.H., Humphries, J.W., & Hamilton, J. A. (2005, June). Survey: Security in the system development life cycle. *Proceedings of the 2005 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY.*

[2] Cannon, David L., Bergmann, Timothy S., & Pamplin, Brady (2006). *CISA Certified Information Systems Auditor Study Guide.* Indianapolis, Indiana: Wiley Publishing, Inc.

[3] Cheriton, D. R., & Faria, D. B., (2006, September). Detecting identity-based attacks in wireless networks using signalprints. *Proceedings of the 5th ACM workshop on Wireless security WiSe '06, ACM Press,* 43-52.

[4] Cooke, E., Bailey, M., Mao, Z. M., McPherson, D., Watson, D., & Jahanian, F., (2004, October 29). Toward understanding distributed blackhole placement. *WORM, ACM Press,* 54-64.

[5] Cox, Mark, (2007, February). Top ten trends among SMBs. *eChannelLine Daily News*, Retrieved February 15 2007, from http://www.echannelline.com/usa.

[6] Criminals increasingly turn to zombie PCs – Microsoft fears the rise of the Botnet. (2006, December 27). *Techworld Kavanagh Report*, Retrieved January 25 2007, from http://www.techworld.com/news/index.cfm?newsID=7674.

[7] De Guzman, Mari-Len, (2005, June 20). Banks to spend more on IT security, survey says privacy regulations and other compliance issues are behind the spending uptick. *IDG News Service*. Retrieved January 25 2007, from http://www.computerworld.com/action/article.do?command= viewArticleBasic&articleId=102642.

[8] Dunn, John E., (2007, January 24). Microsoft Holds Botnet Summit – Secret Squirrels Mull Security Threats. *Techworld Kavanagh Report*. Retrieved January 25 2007, from http://www.techworld.com/news/index.cfm?newsID=7835.

[9] Grance, T., Hash, J., & Stevens, M. (2003, October). Security considerations in the information systems development life cycle. *NIST Special Publications 800-64.*

[10] Hansche, S., Berti, J., Hare, C., (2004). *Official (ISC)2 Guide to the CISSP Exam.* Boca Raton, Florida: Auerback Publications.

[11] Lam, V. T., Antonatos, S., Akritidis P., & Anagnostakis, K. G., (2006, October). Puppetnets: Misusing web browsers as a distributed attack infrastructure. *Proceedings of the 13th ACM Conference on Computer and Communications Security CCS '06, ACM Press,* 221-234.

[12] Lee, C. P., & Copeland, J. A., (2006, November). FlowTag: A collaborative attack analysis, reporting, and sharing tool for security researchers. *Proceedings of the 3rd International Workshop on Visualization for Computer Security VizSEC '06, ACM Press,* 103-107.

[13] Moffie, M., Cheng, W., Kaeli, D., & Zhao, Q., (2006, October). Hunting Trojan Horses. *Proceedings of the 1st Workshop on Architectural and System Support for Improving Software Dependability ASID '06, ACM Press,*
12-17.

[14] Orgill, G. L., Romney, G. W., Bailey, M. G., & Orgill, P. M., (2004, October). The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. *Proceedings of the 5th Conference on Information Technology Education CITC5 '04, ACM Press,* 177-181.

[15] Rode, J., Johnansson, C., DiGioia, P., Filho, R. S., Nies, K., Nguyen, D.H., Ren, J., Dourish, P., & Redmiles, D., (2005, July 12-14). Seeing further: Extended visualization as a basis for usable security. *Symposium on Usable Privacy and Security, SOUP*, 145-155.

[16] Sadasivam, K., Samudrala B., & Yang,T. A., (2005, April). Design of network security projects using honeypots. *Journal of Computing Sciences in Colleges*, Volume 20 Issue 4, 282-293.

[17] Security issues are eroding trust in online banking, survey shows. (2007, January 29). Retrieved January 30 2007, from http://www.digitaltransactions.net/newsstory.cfm?newsid=1232

[18] Tevis, J. J. & Hamilton, J. A. (2004, April). Methods for the prevention, detection and removal of software security vulnerabilities. *ACM Southeast Conference '04, ACM Press,* 197-202

[19] Tupakula, Udaya Kiran & Varadharajan, Vijay, (2006). Analysis of traceback techniques. *Conferences in Research and Practice in Information Technology, CRPIT,* Volume 54.

[20] Wang, A. J. A., (2005, March). Information security models and metrics. *43rd ACM Southeast Conference*, *ACM,* 2:178
184.

[21] Zhang, L., (2003, September). Why do people attack information? And what will be the trend in the future? Department of Computer Science, University of Helsinki, Finland, 1-5. Retrieved January 25 2007, from http://www.cs.helsinki.fi/u/lamsal/ teaching/autumn2003/student_final/lili_zhang.pdf.