Los Alamos
NATIONAL LABORATORY
EST.1943

LA-UR-15-21507
Approved for public release; distribution is unlimited.

Title:	CS651 Computer Systems Security Foundations 3d Imagination Cyber Security Management Plan
Author(s):	Nielsen, Roy S.
Intended for:	submission to academia.edu
Issued:	2015-03-02

Disclaimer:
Los Alamos National Laboratory, an affirmative action/equal opportunity employer,is operated by the Los Alamos National Security, LLC for the National NuclearSecurity Administration of the U.S. Department of Energy under contract DE-AC52-06NA25396. By approving this article, the publisher recognizes that the U.S. Government retains nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Departmentof Energy. Los Alamos National Laboratory strongly supports academic freedom and a researcher's right to publish; as an institution, however, the Laboratory does not endorse the viewpoint of a publication or guarantee its technical correctness.

CS651 Computer Systems Security Foundations
3d Imagination Cyber Security Management Plan

Roy Nielsen

2015 January 10

Table of Contents

Introduction to Information Security

Background on 3d Imagination

3d Imagination is a new company that bases its business on selling and improving 3d open source related hardware. The devices that they sell include 3d imagers, 3d printers, pick and place machines and laser etchers. They have a fast company intranet for ease in sharing, storing and printing large, complex 3d designs. They have an employee set that requires a variety of operating systems including Windows, Mac and a variety of Linux both for running business services as well as design and test machines. There are a wide variety of private networks for testing transfer rates to and from the 3d devices, without interference with other network traffic. They do video conferencing conferencing with customers and other designers.

One of their machines is based on the project found at `delta.firepick.org`(Krassenstein, 2014; Biggs, 2014), which in future, will perform most of those functions. Their devices all include embedded systems, that may have full blown operating systems. Most of their systems are designed to have swappable parts, so when a new technology is born, it can be quickly adopted by people with 3d Imagination hardware.

This company is producing a fair number of systems and components, however to get the funding they need to mass produce quality parts, so they are preparing for an IPO to raise the funds they need. They would like to have a cyber-security audit performed so they can give their investors confidence that they are protecting their data, customers information and printers in a proactive manner.

Background on Cyber Security

3d Imagination has a more and more common situation where they need to not only protect their business systems, but also figure out what level of security to provide customers a way to protect their devices. Just as with normal business security, device security for customers is also like a game of leapfrog(Conway, 2014), not only to keep devices secure, but functional as well(National Cybersecurity and Communications Integration Center, n.d.). There are multiple attack vectors that can be exploited for a company that has this profile. Some common ones are social engineering, network based vectors and personnel bringing on devices that either may be infected or otherwise have malicious code automatically executed when inserted into a system.

Challenges for Consultants on Site

This company is very open about its operation and designs, as the primary products are open source hardware and software devices. The primary concern is to not halt either business or design operations due to normal cyber security auditing and penetration testing. There is always a challenge fitting in a full suite of network, documentation and social engineering auditing to insure there is enough coverage for the customer to feel their money is well spent as well as give them enough information to ensure continued security. A planning session will take place while on site to discuss future plans to keep customers systems secure so as to not find themselves victim of malicious attack as printer and batteries have been in the past(Brodkin, 2010). A final portion of the site visit will be reporting the findings to the security personnel and management of the company and offering suggestions for potential improvement.

Current Challenges for 3d Imagination

3d Imagination has a challenge with open source business model. They must make sure that potentially submitted code and designs have security in mind, with no malicious features or unsecure features that could leave systems open to easy exploit. Their primary concern right now is gearing up for their IPO, for business, design and manufacturing. If security is properly embedded into these processes, their transition through post-IPO should be smooth. Spending time on a plan to provide secure firmware, operating systems and software support to customers is a concern because it can be easy for this process to become prohibitively costly, if not managed carefully. Initial recommendations going into the audit would be to limit the supported operating systems and software packages so providing updates is more realistic. Setting up automated build and test environments in a Continuous Integration(CI) setup can also help minimize bugs and security vulnerabilities(Stiehm & Gotimer, n.d.).

Security Assessment

Asset Description

3d Imagination has split their organization into five different groups. Although they have one flat company network, asset descriptions will follow along these lines. The table below gives a brief description how these groups are organized, and the assets as well as function each group contains.

Operations	Function	Operating Systems	Systems Description
External Business	Web store services	Linux	Apache, Mysql , Php
Internal Business	Oracle Enterprise Planning	Oracle Linux	Oracle DB and Web Services
Internal Engineering	Workstations	Windows, Linux, Macs,	3D Design, Electronics prototyping, Embedded System Design
Internal Prototyping	Workstation & embedded systems	Linux & Mac	Rework, Redesign, Debugging, Systems Prototyping
Test and Validation	Workstations, Embedded, 3D Devices	Windows, Linux, Mac	Engineering, Prototyping, Continuous Integration, Physical Assembly

Table 1: Organizational Assets

Risks of no network segments

> In cyber security, overall security is only as strong as the weakest link...(Sunguard Cyber Security, 2010)

All devices are connected to the same network, there is no segregation or separation into separate networks based on functionality or systems description as described in the table 1 above, as suggested by the NSA(niasc@nsa.gov, 2013). In the case of 3d Imagination, main problem is that all eggs are in one basket, and the security as stated above '...is only as strong as the weakest link...'. Once the weakest link is compromised, it is used as a foothold to launch more sophisticated attacks towards higher value targets(CANSO, 2014). A flat network such as this one is highly discouraged. It is recommended that alternatives to a flat network be planned implemented.

Targeted Risks

The functions in table 1 are organized such a way as to segregate the services or functionality in the systems description to be able to have separate security domains. Each has a different method or attack vector for attempted exploitation. For external web stores, black hats(Gibson, 2010) know to specifically target web servers, databases and the languages or methods used in programming the web interface. For internal business systems, the primary industry standard is to use a database, connected to some kind of web service. If a little bit of research is done on the company as a target, a black hat will know what to target in the way of engineering, prototyping and validation systems. One over arching attack vector is a port scan that will make an attempt to perform an 'OS fingerprint'(Schwartzenberg, 2010) to determine what operating systems is being used on a machine, so as to choose specific vulnerabilities to target.
These types of attacks can be defended against in a variety of ways, and if they are not found in the organization, recommendations to mitigate these risks will be documented and discussed in the contractor exit interview.

Assesing Risks

The Targeted Risks section covered one aspect of how we will be testing the security of 3d Imagination. We will also audit documentation to determine if the controls meet national standards, specifically NIST(Dempsey, 2014; Joint Task Force, 2013) and CIS guidance(*The CIS Security Metrics*, 2009). Other organizations that provide guidance include NSA(*About IA at the NSA*, n.d.), DISA(*Security Technical Implementation Guides (STIGs)*, n.d.) and operating system vendors.

Mitigation of Risks

After assessing the risks of 3d Imagination, we will report the results of our findings as well as methods to protect the organization in layers of protection, much like one would find in an onion or set of russian dolls(Papallo, 2008). Some standard recommendations we use include separation of duties of machines on the network, with different networks for the different functionality the business requires. Another recommendation will be to standardize the format and outline of documents such as set up and operations guides for services and networks. These should follow national industry standard guidelines at a minimum and provide more protection if possible. As an organization that may become a target, we would also recommend setting up internal audits at least yearly with regular external audits as well to have a 3rd party determination score the readiness of the organization.

Access Controls and Security Mechanisms

Access controls and security mechanisms are important for all aspects of the company objectives. However, unlike in the previous section, we will also consider making sure the the shipped products also have access controls and security mechanisms available. There are many variations on authentication mechanisms used to authenticate to a website on the Internet. The methods used for authentication can fall in a few categories(Smart Card Alliance, 2012), generally some confidence, high confidence and very high confidence. Three factor authentication is in the very high confidence category. Three factor Authentication is defined as something a person knows, something a person has and something a person is. Something a person knows would be a password, something a person has would be a smart card or smart token and something a person is would be something like a fingerprint or iris scan(Yu, 2014; Reno, 2013). The NSA has provided a brief tech note called 'Hardening Authentication'(The Mitigations Group, 2012), that can be used to harden authentication systems.

Needed Access Control Mechanisms

In the above asset description section, the business was split into several business sections describing the different functions in the organization. These business sections may have varying authentication needs. Later we will discuss splitting the company internet along the lines of these business sections. Each section may have a different set of users, and some users may be members of multiple sections. Segregating authentication and networking based on business section provides better security via the principle of least privilege(Krohn, 2005).

Another important part of authentication is logging all authentication events, both successful and unsuccessful. This can be very valuable when trying to determine the cause or path of attempted incident.

External Web Store Services

The external web store can have SSL/TLS based authentication. Some sites have 'Remember Me' technologies where a cookie is stored on the system to show the site the user is already logged in. 'Remember Me' technology is not considered very secure(Karlof, 2009). It may be worth considering to have a time limitation on the stored cookie to limit the time the login cookie is valid.

Internal Enterprise Resource Planning

The internal Enterprise Resource Planning services handle central services including finance and human resources. This information is essential to the success of the company from a business perspective. We recommend at least two factor authentication for access to these resources. Access should be limited to least privilege, where employees only have access to what they need to perform their job function. Maintainers of the ERP should have higher privilege to resources than employees that have no need to access business resources other than to track their time.

Internal Engineering, Prototyping as well as Test and Validation

These sections should all have similar authentication mechanisms, but authorization via authentication should not cross boundaries between these business units. Internal Engineering is primarily where the designs of systems are performed. Although Prototyping may feed back into Engineering, it is recommended to have Prototyping as a separate unit as Engineering's purpose is to design to specifications, where as Prototyping has more of a research and development role. Testing and Validation should be like a third party entity that had no hand in design or prototyping to prove that the design of the unit is fully functional and ready for customer use.

End Products

The end products of this company include embedded computer systems. Designs should include easy to set up and configure authentication mechanisms to prevent embedded hack attacks such as has happened to Hewlett Packard in the past(National Cybersecurity and Communications Integration Center, n.d.; Brodkin, 2010). Set up guides should have well documented security controls including how to keep the device's operating system and software up to date.

Network Protection through Access Control

As briefly touched on above, any way to ensure the principle of least privilege when accessing resources can increase the security of the internet.

Network Segments

One primary way to do this is through giving access to employees only what they need to complete their job function. Segregation of the internet into separate networks helps compartmentalize security and help limit what employees have privilege to access, limiting the potential for a security breach. Some employees may need access to resources on more than one network, but that can be managed by a central authentication mechanism that gives rights to access resources on the company's internet.

Customer Education

We recommend providing a brief introduction to system security to customers with specifics on how it pertains to their new devices. This can help protect customers from potential hacks or attacks like those suffered by Hewlett Packard customers.

Single Sign On and Vertual Private Network Integration

Single Sign On or SSO provides an authentication mechanism where an employee can log in once and have access to all the resources that employee needs(D'Costa-Alphonso, 2010). This kind of authentication service could make access to segregated resources as recommended above transparent to the employee. Virtual Private Networks or VPNs can provide secure access to internal company internet by employees on the Internet(Netgear, 2005) working from home, collaborating at another company's site or from a conference. Coupling the two technologies can provide secure transparent access to allow for a mobile workforce with secure access to business resources.

Security Policies, Procedures, and Regulatory Compliance

The upcoming IPO presents a more focused view of the company from investors and regulators. To make sure the company can stand up to the increased scrutiny, management needs to have a basic understanding of regulations, document corporate cyber security policies as well as implement controls to satisfy the policies and regulations. Solid documentation, policies and processes will need to be in place to provide the level of confidence you will need the investors to have to encourage purchase of company shares. One example is protection of data both at rest and in transit.

Regulatory Responsibilities

While there are several laws that the company is required to follow, it is also recommended that the company also follow some laws that my be implemented only in some states, or possibly other countries(CSO Staff, 2012). Following these extra rules not only provide an ability for future expansion, but could also lower risk of penalty from governmental fines or lawsuits.

Laws the company will be required to follow include:

- Sarbanes-Oxley Act (SOX)
  - Specifies disclosure and transparency rules to both the public and investors.
  - Also specifies rules for records retention and auditing.
- Payment Card Industry Data Security Standard (PCI DSS)
  - Customer payment data is protected by this law. Any transport or recording of the data must be protected.
- Fair and Accurate Credit Transaction Act (FACTA), including Red Flags Rule
  - Helping customers avoid Identity Theft. Companies must protect and dispose of customer information properly.
  - Red Flag Rule: New requirement to implement identity protection program.
- Federal Rules of Civil Procedure (FRCP)
  - Governs civil court procedures.
  - Includes rules for good stewardship of electronic data

It is recommended to follow these laws and regulations. Following these now as well as providing transparency into these business practices may provide an easier transition to international trade, as well as help to induce high customer and investor confidence in the company.

- Free and Secure Trade Program (FAST)
  - Voluntary supply chain certification program
- Customs-Trade Partnership Against Terrorism (C-TPAT)
  - Voluntary supply chain security certification program
- Massachusetts 201 CMR 17 (aka Mass Data Protection Law)
  - Law establishing a framework for protecting customer data from identity theft
- Nevada Personal Information Data Privacy Encryption Law NRS 603A
  - Requires encryption of customer data both in trasit and at rest.
- Law on the Protection of Personal Data Held by Private PartiesMexico
  - Company must have lawful reasons for collecting personal customer data. Customers must be notified if information is breached.

Company Policies to Fulfil Responsibilities

Individual policies that spell out procedures for handling information security can help fulfill some of the legal requirements for some of the above laws. The following is a straw man outline for policies should be defined for a company in this business. These policies should be defined by management with some legal assistance.

- Personal Electronic Devices (PED)
  - How does the company handle company data on personal devices, such as cell phones, tablets, laptops, computers, other embedded devices, such as 3d printers.
- Acceptable Use
  - Specify rules for use of company computing devices
  - Specify rules for use of company network
  - Specify rules of use for company resources off-site
- Handeling of Customer Data
  - Rules for data in transit
  - Rules for dat at rest

- Records Retention
  - Retention of customer data
  - Retention of the business financial data
  - Retention of email
  - Retention of customer support transactions
  - Retention of server and service logs
- Identity Protection
  - Protection of customer identity
  - Protection of employee identity
- Server, Service and Project Computing Security
  - All server, service and project computing resources will have a computing security plan. Templates will be made available.
  - Every internal and external audit shall feed back into active change of company policy.
- Data Encryption
  - Encryption of customer data at transit
  - Encryption of customer data at rest
  - Encryption of business sensitive data in transit
  - Encryption of business sensitive data at rest

Controls to be Implemented

There are many controls that should be implemented to protect company and customer data. As discussed before, information security is like an onion or russion doll - each layer of security provides protection. Three specific controls that can be implemented to provide an implementation to company policies described above include setting up systems per recommended security settings, control of PEDs and implementing a central logging system.

System Security Settings

In the United States, government agencies are required to minimally follow the information security standards defined by the National Institute of Standards and Technology(NIST). There are also other government and industry standards set by the Department of Defense(DOD), National Security Agency(NSA) and the Center for Internet Security(e CIS) that may have a more strict or equivalent approach to NIST guidance. These organizations have documentation on securing many operating systems including mobile, workstation and server systems. Documentation such as a setup guide and possibly

checklist should be developed by information security professionals and implemented by IT to ensure security standards are met. These company documents need to be developed such that secured systems are both usable and secure. Some security settings can be draconian and make systems hard to use, so a risk based approach needs to be taken to analyze industry guidance to make sure regulations are satisfied, but employees are not hampered from doing their job.

PED control

Intentional and unintentional use of PEDs can be a successful attack vector that can compromise any part of the business. Mobile devices are being made more and more user friendly, as well as making employees more efficient and highly effective. PEDs can range range from any peripheral that can be plugged into a computer, to laptops, phones and tablets. These systems can host some malicious software that can compromise the security of your computers and computing infrastructure, leading to customer and business sensitive data loss. One option is to provide all the mobile devices required to perform the job, making sure the systems are configured and maintained to industry security standards. There are other ways to manage PEDs, or even make the choice to not manage them. A risk based decision needs to be made by management, having been given a recommendation from company information security.

Robust Central Logging

There are several products both commercial and open source that will collect the logs from all company systems, retain the logs and filter them to look for specific events. Analyzed logs can be used to look for server, application or workstation problems or bugs that may degrade system performance as well as do the same for security. This service is essential to a healthy company network, and management must make a decision as to what product it will use rather than if it wants to employ this measure. These systems can include mechanisms to insure retention of logs that may have legal importance, satisfying regulatory requirements.

Protecting Data at Rest and in Transit

There are two states that data can be view, being in transit between systems, or stored on disk or other media. By default, most servers and services provide thier material by way of clear text, making the data available to anyone who has access.

Protecting Data at Rest

Data saved on a hard drive is normally viewable by anyone that has access to the system. Law requires that we protect customer data. Business sensitive data also needs to be protected against theft. Following the principle of least privilege, we only want people to have access to that data that require it to fulfill their company business function. Encrypting the data when a machine is off means that if anyone turns on the machine, they are required to provide some kind of security code to access that data when the

machine is turned on again. If a physical machine is stolen, a thief would not be able to access the data, thus adding a layer of security to our russian doll that protects company data. This will make it much harder for those that may have malicious intent that do not have access to the data, whether they are internal or external to the company.

Protecting data in transit

Unfortunately any information not deliberately protected on the network is available to anyone that has access to the wires transmitting the data. Data in transit is transmitted in clear text, easily read by anyone with access to the same network, or a location in between. Encryption provides protection of the data in between two end points that are communicating with each other. For web traffic, the recommendation is to use HTTPS rather than HTTP, as HTTPS provides encryption of data at the transport layer. At the hardware level, networks can be set up to provide IPSEC(Sridevi, 2014) to protect all network traffic. This double protection provides two layers of security, if one were to fail, the other could provide the needed protection. Other transfer methods can be re-directed over network ports that provide encryption as part of the protocol. An example would be to use Secure File Transport Protocol(SFTP) that uses Secure Sockets Layer(SSL), rather than the rather aging clear text File Transport Protocol(FTP). The company information security professionals should be well versed on protection of data in transit.

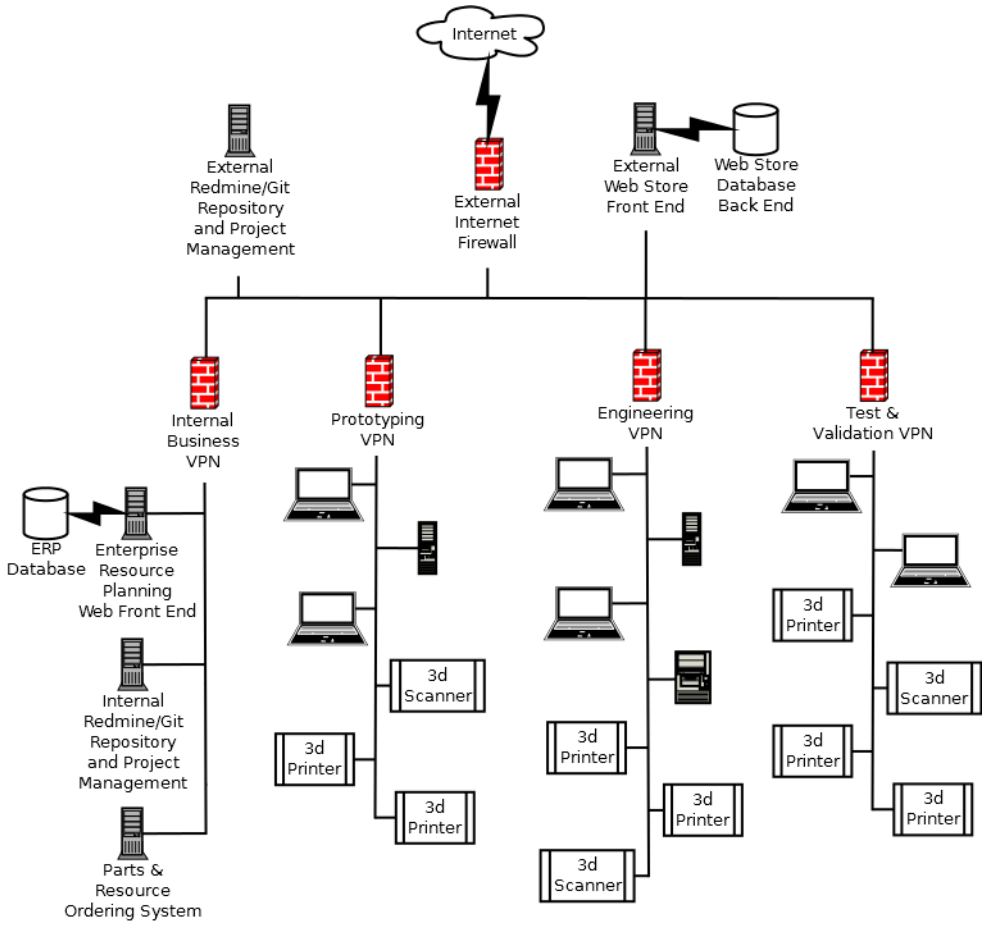
Network Security

The very first step is to redirect all network traffic through a single point and only open the ports on the firewall necessary for business traffic. This will need to be kept current as technologies are constantly being developed and evolving and you want to keep up with new technology. Another first step to securing the company's network is providing VPN support. Every network needs both reactive and active protection protection through Intrusion Detection Systems(IDS) and Intrusion Prevention Systems(IPS).

Proposed Network

The proposed network has the structure found in figure 1.

Figure 1: Recommended Network Structure



Access Controls

One of the principles of information security is separation of duties(Swanson & Guttman, 1996). Authentication and authorization systems should also give access in a way that gives access to only those business resources needed to perform ones duties. This is called least privilege(Swanson & Guttman, 1996). To be able to provide these security boundaries, a company needs to figure out how to logically separate their network into business tasks suitible to map the least privilege principle. In figure 1, we outline this separation via virtual private networksVPN. Some employees may need access to multiple network sections, but again, they should only get access to what they need to perform their job. A VPN also gives the workforce mobility to move offices and be able to work off site and at customer locations, while keeping the network and resources secure. Separation of duties

Intrusion Detection Systems(IDS) and Intrusion Prevention Systems(IPS)

IDS and IPS systems are essential to protecting the network. An IDS is meant to detect attack. An IPS is an IDS that also prevents the detected attack from taking place(Alexander, 2009).

IDS and IPS in Network Operations

An example of how an IDS and IPS works follows. The company IDS detects a port scan on an internal network, such as the Engineering subnet. The IPS will can be set up to block that machine from the network. The two work in concert to protect the company network. These systems need to be well supported as the methods and mechanisms of attacks are constantly evolving. A maintained support contract for both IDS and IPS is highly recommended.

References

About ia at the nsa (Tech. Rep.). (n.d.). National Security Agency. Retrieved 2015 January 21, from https://www.nsa.gov/ia/ia_at_nsa/index.shtml

Alexander, J. (2009, September 31). *Intrusion detection and prevention systems (ids/ips)* (Tech. Rep. No. NPFIT-FNT-TO-INFR-0068.01). Retrieved 2015 January 9, from http://systems.hscic.gov.uk/infogov/security/infrasec/gpg/intrusion.pdf

Biggs, J. (2014, June 10). *The open-source electronics robot, the firepick delta, could bring real manufacturing to the desktop* (Tech. Rep.). Tech Crunch. Retrieved 2015/1/13, from http://techcrunch.com/2014/06/09/the-open-source-electronics-robot-the-firepick-delta-could-bring-real-manufacturing-to-the-desktop/

Brodkin, J. (2010, March/April). *Hp printers can be remotely controlled and set on fire, researchers claim (updated)* (Tech. Rep.). ars technica. Retrieved 2015/1/13, from http://arstechnica.com/business/2011/11/hp-printers-can-be-remotely-controlled-and-set-on-fire-researchers-claim/

CANSO. (2014, June 12). *Canso cyber security and risk assessment guide* (Tech. Rep.). Civil Air Navigation Services Organisation. Retrieved 2015 January 19, from https://www.canso.org/sites/default/files/CANSO%20Cyber%20Security%20and%20Risk%20Assessment%20Guide.pdf

The cis security metrics (Tech. Rep.). (2009, May 11). Center for Internet Security. Retrieved 2015 January 21, from https://buildsecurityin.us-cert.gov/sites/default/files/CIS_Security_Metrics_v1.0.0.pdf

Conway, J. (2014, May 20). *Cyber security: Not really a race, more like leapfrog!* (Tech. Rep.). SudoSecure. Retrieved 2015/1/13, from http://www.sudosecure.com/cyber-security-really-race-like-leapfrog/

CSO Staff. (2012, December 19). *The security laws, regulations and guidelines directory* (Tech. Rep.). CSO Online. Retrieved 2015 February 1, from http://www.csoonline.com/article/2126072/compliance/the-security-laws--regulations-and-guidelines-directory.html

D'Costa-Alphonso, M., Marise-Marie; Lane. (2010). *The adoption of single sign-on and multifactor authentication in organizations - a critical evaluation using toe framework*

(Tech. Rep.). Issues in Informing Science and Information Technology. Retrieved 2015 January 27, from http://iisit.org/Vol7/IISITv7p161-189DCosta788.pdf

Dempsey, G. R. D., Kelly; Witte. (2014, February 19). *Summary of nist sp 800-53 revision 4, security and privacy controls for federal information systems and organizations* (Tech. Rep. No. 800-53 overview). National Institute of Standards and Technology. Retrieved 2015 January 19, from http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800-53r4_summary.pdf

Gibson, S. R. (2010, March). *Protect your intangible assets* (Tech. Rep.). For The Defense. Retrieved 2015 January 20, from http://dritoday.org/articles/2010/03_March/FTD-1003-Gibson.pdf

Heyman, B. B. C. J.-N. M. B. K., David; Patel. (2005). *The still untrodden heights: Global imperatives for space exploration in the 21st century* (Tech. Rep.). Human Space Exploration Initiative Center for Strategic and International Studies. Retrieved 2015 January 17, from http://csis.org/files/media/csis/pubs/suth.pdf

How Do You Measure the ROI of IT Management and Monitoring (Tech. Rep.). (2014). solarwinds. Retrieved 2015 January 17, from http://web.swcdn.net/creative/pdf/Whitepapers/npm_roiwhitepaper_130502.pdf

Joint Task Force. (2013, April). *Security and privacy controls for federal information systems and organizations* (Tech. Rep. No. 800-53 rev 4). National Institutes of Standards and Technology. Retrieved 2015 January 19, from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Karlof, C. K. (2009, February 6). *Human factyors in web authentication* (Tech. Rep. No. UCB/EECS-2009-26). Electrical Engineering and Coomputer Sciences, University of California at Berkeley. Doctoral dissertation. Retrieved 2015 January 27, from http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-26.pdf

Krassenstein, E. (2014, June 10). *Firepick delda 3d: One step closer to desktop electronics manufacturing* (Tech. Rep.). I CONNECT007, Connecting The Global Electronics Supply Chain. Retrieved 2015/1/13, from http://www.pcb007.com/pages/zone.cgi?artcatid=0&a=101046&artpg=1&artid=101046&pg=2&_pf_=1

Krohn, P. F. C. K.-F. K. E. M. D. M. R. O. M. V. S. Z. D., Maxwell; Efstathopoulos. (2005). *Make least privilege a right (not a privilege)* (Tech. Rep.). Retrieved 2015 January 27, from http://www.scs.stanford.edu/~dm/home/papers/krohn:least-privilege.pdf

National Cybersecurity and Communications Integration Center. (n.d.). *Multifunction printer vulnerabilities* (Tech. Rep. No. 1-0012-NCCIC-130020120223). Department of Homeland Security. UNCLASSIFIED: National Cybersecurity and Communications

Integration Center Bulletin. Retrieved 2015/1/13, from https://msisac.cisecurity.org/resources/reports/documents/A-0012-NCCIC-130020120223MFPVulnerability.pdf

Netgear. (2005, October). *Virtual private networking basics* (Tech. Rep.). Retrieved 2015 January 27, from http://documentation.netgear.com/reference/nld/vpn/pdfs/FullManual.pdf

niasc@nsa.gov. (2013, October). *Segregating networks and functions* (Tech. Rep. No. MIT-012FS-2013). National Security Agency. Retrieved 2015 January 20, from https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_SegregatingNetworksAndFunctions_Web.pdf

Papallo, A. (2008). *Security onion gives heartburn to hackers: A new approach to secure publishing* (Tech. Rep.). Eurofield Information Solutions. eComPress. Retrieved 2015 January 21, from http://www.eis-usa.com/pdfs/eComPress%20Security.pdf

Reno, J. (2013, August). *Multifactor authentication: Its time has come* (Tech. Rep.). www.timereview.ca, Technology Innovation Management Review. Retrieved 2015 January 27, from http://timreview.ca/sites/default/files/article_PDF/Reno_TIMReview_August2013.pdf

Schwartzenberg, J. (2010, August 12). *Using machine learning techniques for advanced passive operating system fingerprinting* (Tech. Rep.). Retrieved 2015 January 20, from http://essay.utwente.nl/59680/1/MA_scriptie_J_Schwartzenberg.pdf

Security technical implementation guides (stigs) (Tech. Rep.). (n.d.). Defense Information Security Agency: Information Assurance Support Environment. Retrieved 2015 January 21, from http://iase.disa.mil/stigs/Pages/index.aspx

Smart Card Alliance. (2012, November). *Strong authentication using smart card technology for logical access* (Tech. Rep. No. ACC-12002). Smart Card Alliance Access Control Council. Retrieved 2015 January 27, from http://www.smartcardalliance.org/resources/pdf/Strong_Auth_WP_FINAL_112112.pdf

Solutions, V. (2008). *Assesing the financial impact of downtime understand the factors that contribute to the cost of downtime and accurately calculate its total cost in your organization.* (Tech. Rep.). Retrieved 2015, January 17, from http://www.strategiccompanies.com/pdfs/Assessing%20the%20Financial%20Impact%20of%20Downtime.pdf

Sridevi, M. D. H. (2014, MarchApril). *Network security comparison between ipsec and gre* (Tech. Rep. Nos. Volume 3, Issue 2). International Journal of Emerging Trends & Technology in Computer Science. Retrieved 2015 February 1, from http://www.ijettcs.org/Volume3Issue2/IJETTCS-2014-03-25-042.pdf

Stiehm, T., & Gotimer, G. (n.d.). *Building security in using continuous integration* (Tech. Rep.). CrossTalk: The Journal of Defense Software Engineering. Retrieved 2015/1/13, from http://www.crosstalkonline.org/storage/issue-archives/2010/201003/201003-Stiehm.pdf

Sunguard Cyber Security. (2010). *Cyber security for state governments, deleware department of technology and information exercise sharpens skills for cyber attack prevention, detection, response, and recovery* (Tech. Rep. No. WPS-037). Sungard Availability Services. Retrieved 2015 January 19, from http://www.sungardas.com/Documents/CyberSecurityforStateGovernment_WPS-037.pdf

Swanson, M., & Guttman, B. (1996, september). *A risk-based approach to segregation of duties* (Tech. Rep. No. Special Publication 800-14). National Institute of Standards and Technology. Retrieved 2015 February 9, from http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

The Mitigations Group. (2012, September). *Hardening Authentication (Revised)* (Tech. Rep.). National Security Agency Information Assurance Mission. Retrieved 2015 January 27, from https://www.nsa.gov/ia/_files/factsheets/IAD_HardeningAuth_PrintFile.pdf

Yu, G. M. Y. G.-W., Jiangshan; Wang. (2014, November 2014 14). *An efficient generic framework for three-factor authentication with provably secure instantiation* (Tech. Rep.). IEEE. IEEE Transactions on Information Forensics and Security. doi: 10.1109/TIFS.2014.2362979