GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

The Case for End Point Visibility

GIAC (GSEC) Gold Certification

Author: Robert Mier, Robert.Mier@cox.net
Advisor: Rick Wanner
Accepted: February 3, 2016

© 2016 SANS Institute, Author retains full rights.

Abstract

With many data breaches in the news, businesses are recognizing that they're at a greater risk of being compromised. These breaches are so damaging that a Presidential executive order was issued. ("Executive Order -- Improving Critical Infrastructure Cybersecurity | whitehouse.gov," 2013) No longer is the business's firewall able provide the needed defenses to ward off the attacks trying to compromise its network. Management is tasking Information Technology (IT) professionals to build cybersecurity programs to ward off these attacks and prevent the business from becoming the next victim of a data breach. Where to start? What steps need to be done and what order? How to measure the effectiveness of the program? Which standards to use? The National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Center for Internet Security (CIS) Critical Security Controls (CSC) can provide a proven vetted model to help your build your cybersecurity program. This paper will utilize the NIST Cybersecurity Framework and the first two CSCs showing how they can be adapted to a business' existing cybersecurity program.

© 2016 The SANS Institute Author retains full rights.

1. Introduction

On February 12, 2013 President Barack Obama issued executive order Improving Critical Infrastructure Cybersecurity, thus, recognizing the "Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity." ("Executive Order -- Improving Critical Infrastructure Cybersecurity | whitehouse.gov," 2013) This signified on a national level the need for businesses and individuals to be more conscious of the importance of protecting Personal Identifiable Information (PII), credit card information, usernames and passwords, and business critical information.

Between 2005 and 2014 "There have been over 300 data breaches involving the theft of 100,000 or more records (that have been disclosed publicly)." (McCarthy, 2014)

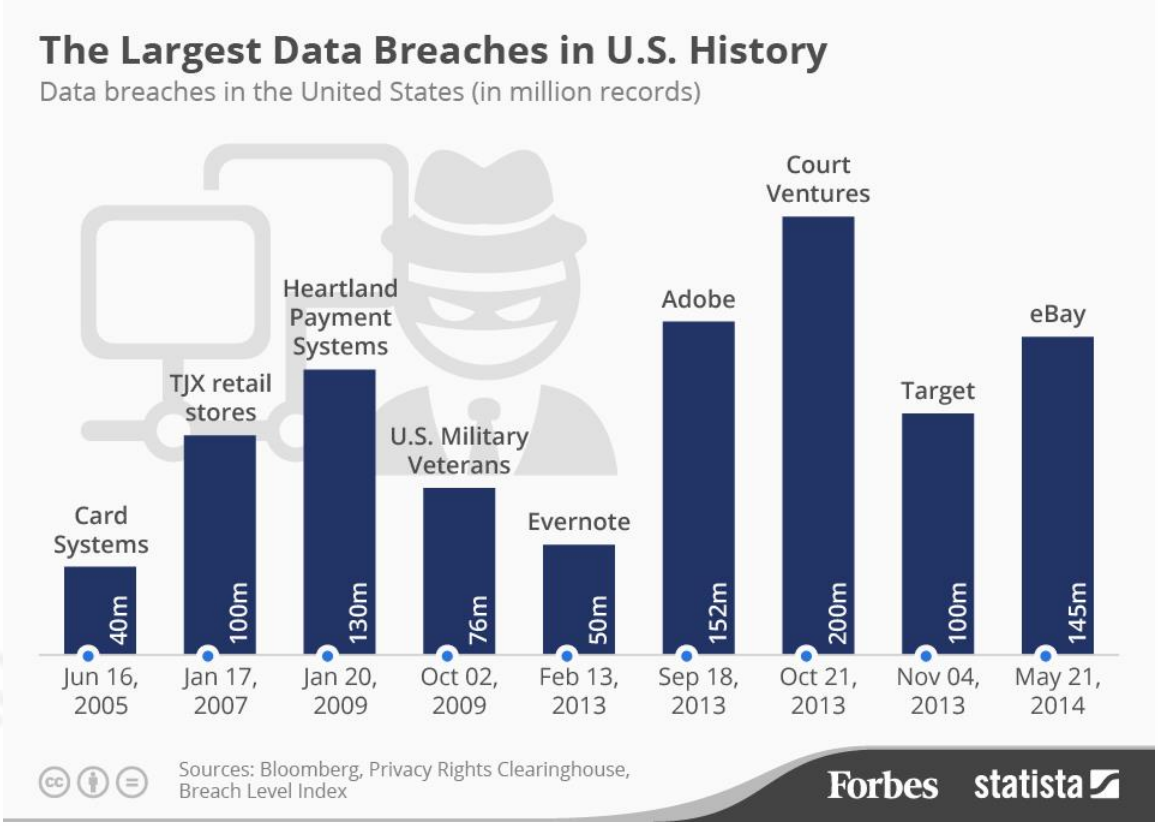


Figure 1: The Largest Data Breaches in U.S. History (Statista. (2014, August 26). *The Largest Data Breaches in U.S. History* [Graph].

Bob.Mier@agvantis.comRobert.Mier@cox.net

© 2016 The SANS Institute Author retains full rights.

As of December 1, 2015, Identity Theft Resource Center (ITRC) has identified 717 breaches which exposed at least 176,275,000 records containing PII were obtained by data breaches. (Identity Theft Resource Center, 2015, p. 22) The cost per record stolen from data breaches has increased to $154 in 2015 from $145 in 2014. (Ponemon Institute, 2015, p. 01) This cost doesn't factor in the damage to the business's reputation, which cannot be fully quantified.

With the prevalence of data breaches and their associated costs, Information Technology (IT) administrators and business executives are becoming aware of the importance of cybersecurity. Cybersecurity policies and procedures help to reduce the risks to the business networks, continuity, and profitability. However, the challenge is in how to implement them into the company.

Leveraging the Center for Internet Security (CIS) IS Critical Security Controls (CSC) and the NIST Cybersecurity Framework this paper will explore the importance these play in the protection of the network and endpoint cybersecurity posture. The CIS Critical Security Controls and NIST Cybersecurity Framework will be introduced and explore how they can work together.

2. CIS Critical Security Controls

From the early 2000's the National Security Agency (NSA) had been collecting information on how cyber-attacks are conducted. With this knowledge the NSA had compiled a list of "controls" that will help mitigate the attacker's ability to perform the attack. The NSA also adopted the "first fix the known bads" (Tom Donahue, CIA) to bring immediate results in reducing vulnerabilities and risk to known attack vectors. With the goal of prioritizing the Department of Defense (DoD) cybersecurity spending, in 2008, the NSA refined this list of controls that were most effective in stopping attacks on the computer infrastructure. (SANS Institute, 2000) At this same time, the NSA was in a "public-private" partnership with CIS and the SANS Institute and agreed to share these controls with the communications, power, and financial sectors. Thus a consortium was created who had the knowledge, expertise, and access to the information gained from past

© 2016 The SANS Institute Author retains full rights.

cyber-attacks. As an extension of this partnership a consortium was expanded to include several others who had "high value analysis" and "after-attack" forensic analysis of the attacker's techniques, tactics, and methods. Thus the Critical Controls were vetted and validated to reduce the vulnerability-based risk that the U.S. Department of State and others had experienced. The complete history of the CIS CSC's can be found at the CIS and SANS Institute's website (HTTPS://www.sans.org/critical-security-controls/hisory).

Armed with these well-vetted controls businesses can assess their current security state. Furthermore, once the business understands their current security state a measureable course of action can be taken to improve their security posture. The CIS Critical Security Controls framework is located at (https://www.cisecurity.org/critical--controls.cfm).

3. NIST Cybersecurity Framework

The NIST Cybersecurity Framework is a three part framework consisting of Core, Profile, and Implementation Tiers. (National Institute of Standards and Technology (U.S.), issuing body, 2014, p. 01) "The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure." (National Institute of Standards and Technology (U.S.), issuing body, 2014, p. 01) Once the business profile is determined, the business is able to effectively apply the Framework Core and Implementation Tiers. The NIST Cybersecurity Framework incorporates many standards, guidelines, and best practices so that businesses can have confidence in and knowing that they are using proven best practices and industry standards that are current and relevant. (National Institute of Standards and Technology (U.S.), issuing body, 2014, p. 01 and p. 02) The NIST Cybersecurity Framework can be found at http://www.nist.gov/cyberframework/index.cfm.

Bob.Mier@agvantis.comRobert.Mier@cox.net

© 2016 The SANS Institute Author retains full rights.

The NIST Cybersecurity Framework is able to allow a business to draw "from those standards, guidelines, and practices" and to leverage the "taxonomy and mechanism" of the framework into their business plan and practices. Businesses will be able to:

> *DESCRIBE THEIR CURRENT CYBERSECURITY POSTURE;*
>
> *DESCRIBE THEIR TARGET STATE FOR CYBER SECURITY;*
>
> *IDENTIFY AND PRIORITIZE OPPORTUNITIES FOR IMPROVEMENT WITHIN THE CONTEXT OF A CONTINUOUS AND REPEATABLE PROCESS;*
>
> *ASSESS PROGRESS TOWARD THE TARGET STATE;*
>
> *COMMUNICATE AMONG INTERNAL AND EXTERNAL STAKEHOLDERS ABOUT CYBERSECURITY RISK.*
>
> *(National Institute of Standards and Technology (U.S.), issuing body, 2014, p. 04)*

Four elements comprise the core of the NIST Framework: Functions, Categories, Subcategories, and Informative References. (National Institute of Standards and Technology (U.S.), issuing body, 2014, p. 07) The framework provides a mechanism to assess the current state, set achievable goals, measure the amount of work to be performed, and present the progress to key internal and external parties.

There are five parts of the Functions element; Identify, Protect, Detect, Respond, and Recover. These provide an outline, model, or stages to help create, guide, or adapt a company's cybersecurity program. These functions are meaningful for more than just the IT department. Through the process of identifying your computers, servers, routers, switches, and other equipment like printers and multifunction copiers an understanding and knowledge of the company's assets are gained. This enables decisions of which items are authorized and which are not authorized. Identifying what is in the company's environment provides information for asset and lifecycle management, IT, management, budget, and planning for future equipment needs to better serve the company's business

© 2016 The SANS Institute Author retains full rights.

plans. The Identify function is also beneficial to the company's Data Loss Prevention (DLP) program by knowing what methods company data can leave. Thus, Identifying IT equipment immediately becomes a value add to the company's Board of Directors, Executive management, finance, and IT department.

Identify leads into the next activity, Protect. Once you know what is in your environment, the business can then make informed decisions on how to best protect its assets thus lowering risk to the business. The NIST Framework which leverages the industry best practices, guides, and standards will be used to assess the current cybersecurity posture and help determine a path to enhance, mature, the cybersecurity posture.

Protect leads into activities to Detect. Detect vulnerabilities, abnormal behavior, internal and external attacks to the company's environment. Visibility enables the business to monitor the environment and to detect when things deviate from normal conditions.

Detection then leads to respond. Now that the business can detect irregularities as they happen in their environment. Detection activities enable the business to initiate mitigation or respond to these abnormalities in a structured response. Mitigating the attack or abnormal behavior in a timely manner also reduces the risk to the business.

After responding to an attack or incident the business then moves into Recover. This is where the business learns from the incident, implements lessons learned, and performs steps to bring the business to a state of normal operations.

Categories divide each of the functions into desired end states. While the subcategories are activities performed by management and IT that when complete support or achieve the goals of the specific category. Informative References are the standards, guides, and best practices from around the industry and government sources. When properly utilized, the references are used to provide evidence of compliance or governance to standards and best practices. These are not all inclusive, nor are they stagnant. Review these periodically for any changes or updates.

Bob.Mier@agvantis.comRobert.Mier@cox.net

© 2016 The SANS Institute Author retains full rights.

NIST Framework is adaptive to the uniqueness of many different businesses' and industries. The Framework can be applied to the existing company cybersecurity program. Many of these steps can and should be performed either concurrently or in parallel. Most of them should be done continually.

The NIST Framework is not meant to be a sprint or quickly accomplished. The pace of the NIST Framework and CIS Critical Security Controls should be adjusted to the current situation and the accepted risk of the business. The business environment and business plans may require a fast tempo in response to mitigate risk or a breach or a slower tempo for normal day to day operations. The NIST Framework can be leveraged to mature the cybersecurity state over a period of time. However, just like the attacks change so must the company cybersecurity program.

4. Where to begin?

Where to begin is to evaluate where the company is at this point in time. This should be an evaluation of the current environment, business continuity plan, IT policies, governance requirements, and company procedures. Armed with this information the environment or equipment in the company would be a good place to start.

CSC 1: Inventory of Authorized and Unauthorized Devices

ACTIVELY MANAGE (INVENTORY, TRACK, AND CORRECT) ALL HARDWARE DEVICES ON THE NETWORK SO THAT ONLY AUTHORIZED DEVICES ARE GIVEN ACCESS, AND UNAUTHORIZED AND UNMANAGED DEVICES ARE FOUND AND PREVENTED FROM GAINING ACCESS. (The Center for Internet Security, 2015, p. 10)

Are assets being tracked? How are assets being tracked? What frequency are assets being inventoried? Are the assets able to be verified by automation? Are all of the audit requirements being meet? Does documented procedures and processes exist? Are there policies to govern and direct the company and are they being reviewed and approved by Executive Management or the Board of Directors?

Bob.Mier@agvantis.comRobert.Mier@cox.net

© 2016 The SANS Institute Author retains full rights.

CSC 1 is referenced in the NIST Framework in the Identify function specifically. CSC 1, though, is a foundation to which other functions in the NIST Framework are built upon. Keeping the ultimate goal for the company, the Cybersecurity program, the initial step, CSC 1, is basic element. The foundation begins to be laid by a good inventory of devices. The second part of is to determine which of these devices are authorized to be on the company network. The cybersecurity program starts to mature from here because once devices are determined to be authorized the other devices then are identified as "Unauthorized". Unauthorized devices then can be identified and removed from the company network.

The decision of which device is authorized and which device is unauthorized has to be based upon company policy. Company management takes part in this by providing policy guidelines to define the cybersecurity program. NIST function Identify categories Business Environment, Governance, Risk Assessment, and Risk Management Strategy address these policies. There are different categories for each function of the NIST framework that should be incorporated. These NIST functions and respective categories should be leveraged to help the IT and executive management craft policies based upon input from industry experts and, best practices. Policies like Bring Your Own Device (BYOD), Wireless Network, Virtual Private Network (VPN), Remote Access, the Cloud. These policies will define what is authorized for the company and what risk tolerance is acceptable to the business.

Although tools are mentioned in this paper, it is outside of the scope to review or recommend any tool(s). Tools are indispensable in any cybersecurity program and the importance of taking the proper amount of time to gain an understanding of what tools(s) best meet the needs of the company and what specific role(s) they will play in the cybersecurity program must be recognized. Whichever tool(s) are employed to detect devices on the network, they should include both active and passive techniques, the ability to scan wired and wireless networks, and be able to monitor any cloud based infrastructure or services. Automation and tools exist in helping establish, monitor, and maintain the cybersecurity program. Some additional feature that are useful when considering a tool and automation selection might include Asset Lifecycle Management,

© 2016 The SANS Institute Author retains full rights.

Network Scanning, Patch Management, Endpoint Monitoring, Vulnerability Management (Malware, Spyware), and Configuration Management integrations. These features are not exhaustive nor considered all inclusive. It is important that these other aspects (Lifecycle and Asset Management, Governance, Business Continuity, Help Desk) be kept in mind when evaluating a tool as it could be a single module in a bigger solution or have to integrate with other solutions that are in use in the company.

CSC 1 addresses detecting devices and determining which are authorized and which are unauthorized. Just as CSC 1 touches many different aspects of the company from risk tolerance, to budget (personnel and tools), to policies and procedures. Knowing what is in your environment is essential. Once this is known and the steps to continuously monitor what devices are authorized and remove those that are unauthorized, the company is ready for CSC 2.

CSC 2: Inventory of Authorized and Unauthorized Software

Actively manage (Inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution. (The Center for Internet Security, 2015, p. 09)

With attackers actively scanning for vulnerable software it is necessary for a company's cybersecurity program to know what software is installed and running on its network. When one system is compromised, it becomes the system that attackers will use to recon the entire company network. Once they learn the layout of the company network attackers then can compromise other systems. These compromised systems become tools for the attackers to compromise other systems, attack other companies, and are used in the exfiltration of sensitive information. In the 2015 Cost of Data Breach Study, is stated that "Malicious attacks can take an average of 256 days to identify while data breaches caused by human error take an average of 158 days to identify." (Ponemon Institute, 2015, p. 03) In either case software vulnerabilities are leveraged. This is the importance

© 2016 The SANS Institute Author retains full rights.

of why inventory of software that is in the company is listed as the second Critical Security Control.

Every device runs one or more pieces of software. Software can be the Operating System (OS), BIOS, and Firmware to applications like word processors, spreadsheets, databases, email, industrial equipment controls, and websites. Each of these could contain vulnerabilities that would allow an attacker to infiltrate the company and take over control of that device.

Just like CSC 1 identifies devices on the network, CSC 2 identifies the software running on each detected device. Knowing what software is present in the company is essential information to the company. It effects the company in several different aspects like risk management, licensing, vulnerability management, Data Loss Prevention. The company policies and directives should guide the evaluation of what software is authorized and which is not authorized.

One concept to classify and handle software is the concept of lists. White Listing, Gray Listing, Black Listing of software should be created and used to determine further actions. Software that is allowed to be used in the company is placed on the white list. Conversely, software that is not allowed should be placed on the black list. Which leads to software that is inherently dangerous if not used correctly. Software that is used in the compiling or decompiling of software, penetration testing, and scanning are examples of some software that should be classified as authorized high risk software and should be placed on the "Gray" list. This type of software should be monitored and restricted to limited named users as they server a valid business use, but can also be used to compromise company assets.

These classifications of the software should also include other details to be included manufacturer, proper name, version, and the hash to name a few details. Tracking these details about software will enable further security aspects like patch management and application monitoring. This information about the software running in the company should be kept current and placed in the company's business continuity documentation and asset management system.

© 2016 The SANS Institute Author retains full rights.

Next step is to find and remove the software that is on the black list. This is an important step. Be on the lookout and aware that during the removal of unauthorized software, some dependencies of authorized software will be revealed. Revelations of these relationships should be documented and utilized to make the determination of whether the software should be paced on the white or gray list and/or if the dependency should be mitigated.

Now that the unauthorized software has been identified, and the process of removal is underway, what is in place to prevent the unauthorized software from being downloaded or from being executed in the company's environment? How is software inventoried? How often does the company network get scanned for software? Does the software inventory system integrate with the hardware inventory system? Tools and automation used to scan the company network can scan for devices and then inventory their hardware and software. Some other equipment like Intrusion Detection Systems (IPS) and Intrusion Prevention Systems (IPS) have the capability to prevent use of unauthorized software from running. Other software can be prevented from communicating with the outside internet by content monitoring and Firewall Access Control Lists (ACLs). Software used for social media, cloud collaboration, file sharing, and streaming media are blocked by the firewall, so that the company's computers and systems cannot reach out to the internet to the internet sites that enable the software to run.

There are several tool suites that have the ability to scan the environment for devices. Once the devices are discovered, they perform a software inventory. They can apply patches or software updates as needed. Some suites can actually block the unauthorized software from being executed on the computers (Application Whitelisting). Theses suites range in size, features, complexity, and costs. Their appropriateness to the business should be determined by the risk management, governance requirements, and budget of the business.

Bob.Mier@agvantis.comRobert.Mier@cox.net

© 2016 The SANS Institute Author retains full rights.

5. A Cybersecurity Program is born

An important aspect of any Cybersecurity program has to consider and address the manpower requirements. This is one area that cannot be understated. The effective cybersecurity program has to have the proper personnel to implement, monitor, respond to and recover from an incident. Proper staffing should be reconsidered at every maturity stage of the cybersecurity program. Consideration should be given to include time needed to implement any change or addition to the cybersecurity program (Policy, procedure, tools, incident response, and recovery actions). In most small companies this person is has other duties to perform along with Cybersecurity. While other companies outsource this function. Still, some companies have dedicated staff and teams dedicated to cybersecurity. Whichever is the situation, the associated risks must be acceptable to the Executive management and the company's Board of Directors.

The techniques used by "Hackers" continue to change in complexity and increase the difficulty in detecting them. This means that the cybersecurity program needs to change as the attack techniques change. In other words, the cybersecurity program has to mature, remain flexible, and adaptable. The NIST framework and the Critical Security Controls provide some meaningful guidance on how to mature, measure, and to focus on each aspect of cybersecurity.

Starting with assessing your current cybersecurity program, then improve it by further leveraging the NIST Framework and the CIS Critical Security Controls. These resources will help provide measureable and reportable steps to help in maturing your cybersecurity program. "A Measured Companion to the CIS Critical Security Controls" provides a list of "measures" with sample criteria to help with each control. ("Measurement Companion to the CIS Critical Security Controls (version 6)," 2015 pg. 04)

These measures are linked to each CSC by a unique ID and to further link to the sub-controls within each CSC. These enable you to evaluate the current state and identify what can be done to mature in that specific area.

Bob.Mier@agvantis.comRobert.Mier@cox.net

© 2016 The SANS Institute Author retains full rights.

Going back to CSC 1, the control is broken down into 6 sub-controls that can be measurements of maturity. Sub-control 1.1 states “Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization’s public and private network(s).” (The Center for Internet Security, 2015, p. 06) Can be measured by “How many unauthorized devices are presently on the organization’s network (by business unit)?” ("Measurement Companion to the CIS Critical Security Controls (version 6)," 2015) The Measurement Companion also give criteria as examples for concise measurements of each sub-control. These are based upon the best practices, governances, and input from subject matter experts that helped create the CSCs and NIST framework. In some instances these “criteria” will not meet the risk tolerance of the company and therefore should be adjusted accordingly. Some companies would be fine with it taking 1 day to detect and remove an unauthorized device from the company network. While other companies would consider 1 hour an excessive risk, thus, unacceptable. This is an example where the business risk tolerance is less than the criteria in the Measurement Companion and needs to be tailored to the business.

CSC sub-control 1.2 further matures the cybersecurity stature by addressing the use of Dynamic Host Configuration Protocol (DHCP). If your company only uses Static IPs then this control doesn’t apply but should be tested to see if an “unauthorized” device is trying to join the network. This also could signify that an authorized device is not properly configured. Which is addressed by “CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers“. (The Center for Internet Security, 2015, p. 12) The same can be said about IPv4 and IPv6. If your company is only using IPv4 then your cybersecurity must scan for any IPv6 configured devices. Otherwise you could overlook an attack surface this could be exploited.

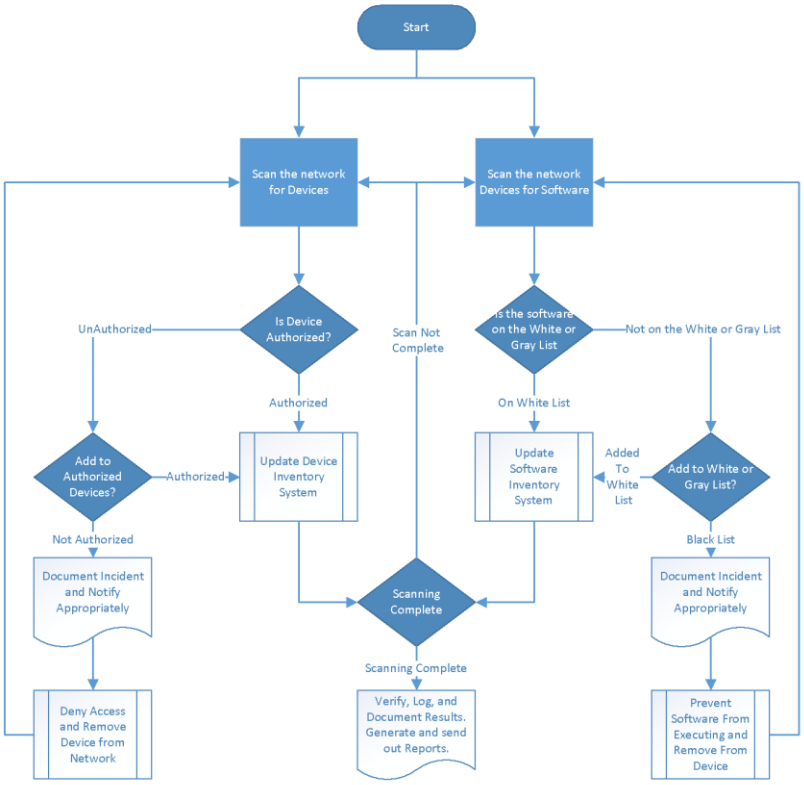
The organization of the CSCs and NIST framework helps companies by focusing in on the Functions and Categories to achieve a robust cybersecurity program that is based upon well-known Informative References. This is where working through the sub-controls of each CSC can help provide a path of measurable steps to mature the cybersecurity posture and program.

Bob.Mier@agvantis.comRobert.Mier@cox.net

© 2016 The SANS Institute Author retains full rights.

6. Cybersecurity Program Execution

The ability to consistently repeat the processes which support the cybersecurity program is key to the effectiveness of the program. The plan needs to be adaptable, easy to communicate, and consistently repeatable. The below process diagram is a high level illustration of one possible scanning process for devices and software that are on the network.



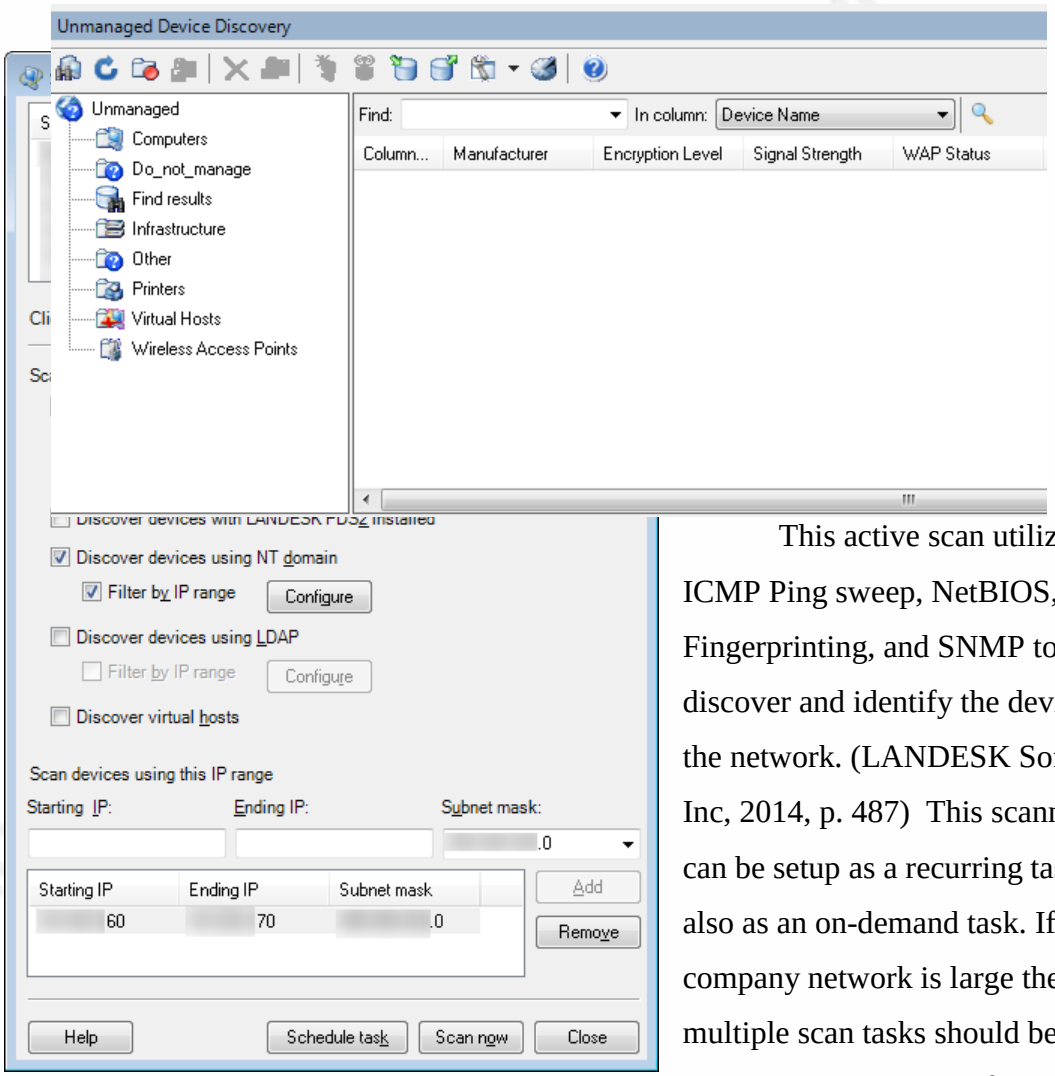
Starting the process are the scanning tool(s) which perform the scan and gather the required information. These tools probe the network and report their findings. These findings must be evaluated and the determination of "Authorized" or "Unauthorized" is made. Evaluating if the unauthorized should be reclassified as Authorized is the next step in the process. Documenting and updating the respective system(s) is then performed before determining if the scans have completely scanned the environment.

Bob.Mier@agvantis.comRobert.Mier@cox.net

© 2016 The SANS Institute Author retains full rights.

One such tool that can be used to accomplished some of the aspects of CSC 1 and CSC 2 is LANDesk Management and Security suite. ("IT Asset Inventory Management | LANDESK," 2016)

The discovery of the devices on the network is accomplished by setting up an Unmanaged Device scan to find IP-enabled devices on the network. This is classified as an ACTIVE scanning technique as the LANDesk core server scans a defined IP range looking for any IP-enabled devices.

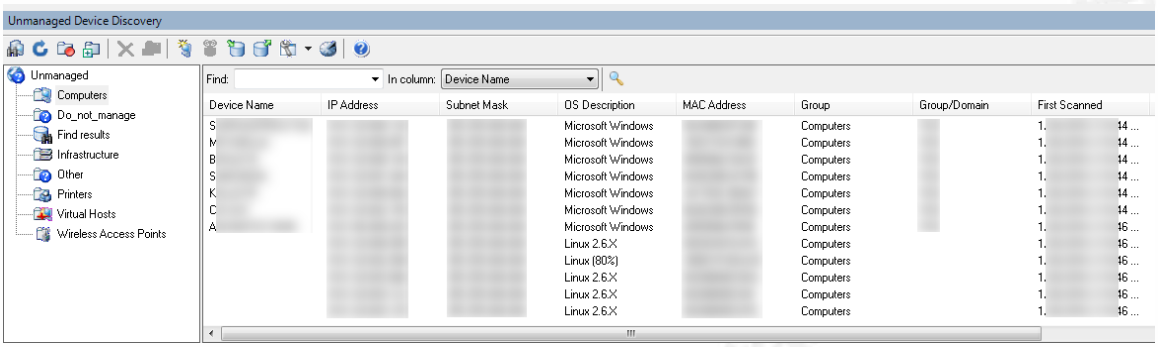


This active scan utilizes ICMP Ping sweep, NetBIOS, IP OS Fingerprinting, and SNMP to discover and identify the devices on the network. (LANDESK Software, Inc, 2014, p. 487) This scanning can be setup as a recurring task and also as an on-demand task. If the company network is large then multiple scan tasks should be setup to scan only a portion of the company network each night. The network can also be scanned on-demand by manually starting the Unmanaged Device Discovery scan task.

Bob.Mier@agvantis.comRobert.Mier@cox.net

© 2016 The SANS Institute Author retains full rights.

After the unmanaged device discovery has completed running the results can be found sorted into the following categories: Computers, Find Results, Infrastructure, Intel vPro, IPMI, Other, Printers, Virtual Hosts, and Wireless Access Points.



Information that is gathered include the Device Name, IP Address, Subnet Mask, Operating System Description, MAC Address, Group/Domain, First Scanned, and more. Passive scanning or identifying what is on the network can also be accomplished with LANDesk utilizing the "Extended Device Discovery" (XDD) tool. XDD relies on a device agent (deployed via an agent configuration) that listens for ARP broadcasts and Wireless Access Points (WAP) signals on the company network. (LANDESK Software, Inc, 2014, p. 488) When a device connects to the network an ARP request is sent out and the XDD device agent will report it to the Unmanaged Device Discovery window of the LANDesk console.

The information this tool provides is useful in identifying what devices are on the network and being able to satisfying, in part or in whole, CSC 1 System sub-controls 1.1, 1.2, and parts of 1.3 and 1.4 as shown below.

© 2016 The SANS Institute Author retains full rights.

The Center for Internet Security Critical Security Controls Version 6.0		
Family	Control	Control Description
		Critical Security Control #1: Inventory of Authorized and Unauthorized Devices
System	1.1	Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.
System	1.2	If the organization is dynamically assigning addresses using DHCP, then deploy dynamic host configuration protocol (DHCP) server logging, and use this information to improve the asset inventory and help detect unknown systems.
System	1.3	Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.
System	1.4	Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.
System	1.5	Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. The 802.1x must be tied into the inventory data to determine authorized versus unauthorized systems.
System	1.6	Use client certificates to validate and authenticate systems prior to connecting to the private network.

Spreadsheet: 1 CSC-CIS Critical Security Controls VER 6.0 Excel 10.15.2015.xlsx

From the gathered information a determination of which devices are authorized and which devices are unauthorized can be made, documented, and steps taken to remove any unauthorized devices from the network. This information can be measured and reported upon. The Center for Internet Security has a Measurement Guide that you can use as a starting point for measuring the risk and effectiveness of the tool being used. The information can also be used to generate reports for management and audits.

CSC 2: Inventory of Authorized and Unauthorized Software (The Center for Internet Security, 2015, p. 03) can be accomplished with the Inventory Scanner and further enabled by another module in the LANDesk Management Suite called Software License Monitoring (SLM). Figure 2 shows the results of the Software Inventory of a computer that was discovered on the network. This is gathered when the LANDesk agent is installed on the computer. This Inventory is gathered automatically by the LANDesk Agent and reported to the LANDesk core server.

Bob.Mier@agvantis.comRobert.Mier@cox.net

© 2016 The SANS Institute Author retains full rights.

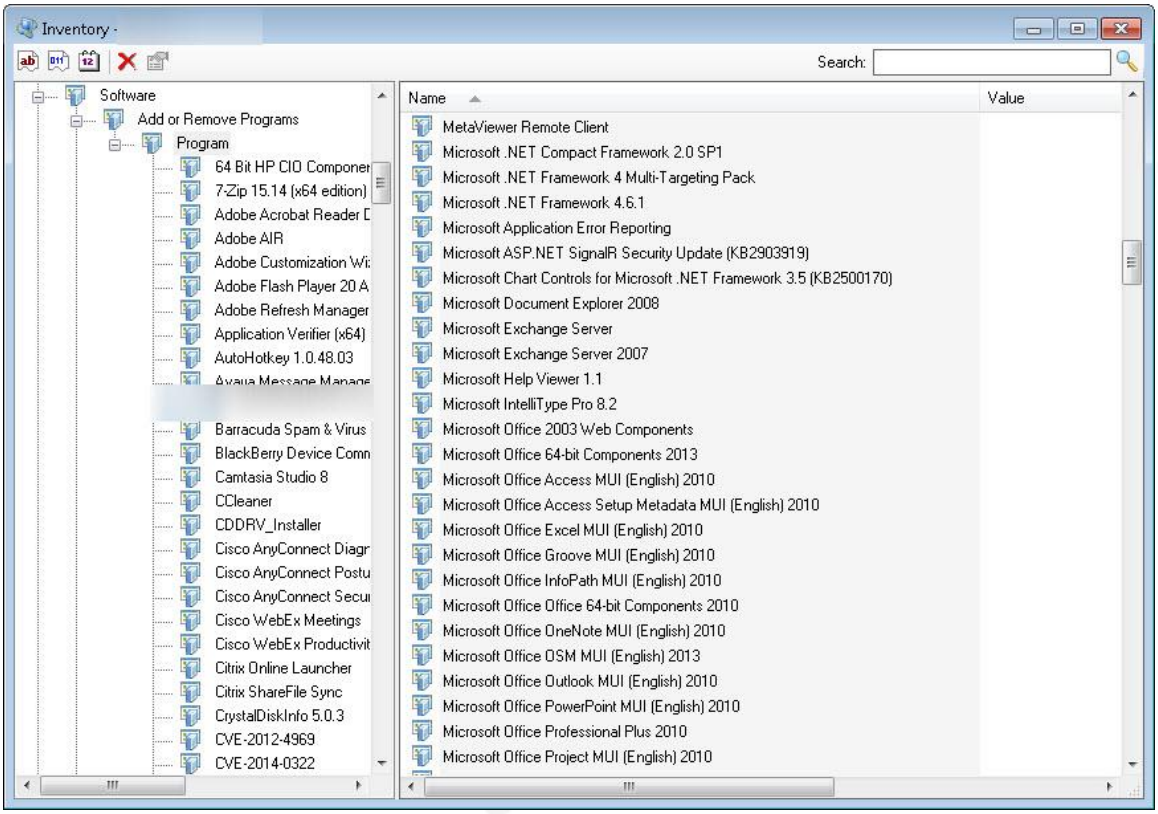


Figure 2: LANDesk Software Inventory Example

This inventory is gathered from all of the computers and servers on the network which the LANDesk Agent is installed. With the reporting capabilities within LANDesk, software is identified and can then be classified as to being authorized or unauthorized. Unauthorized software can then be set to send an alert, can be tracked to the computer(s) or server(s), removed, and set to be blocked by the application control client feature of the LANDesk agent.

Software License Monitoring takes the information gathered by the Inventory scanner and adds the capability to incorporate Software Licensing information and Usage information to better understand what software is being used, how frequently, how many are licensed, or unlicensed. Usage information then can be utilized to manage product licensing and licensing costs associated with the software that is installed on the devices in the company.

Bob.Mier@agvantis.comRobert.Mier@cox.net

© 2016 The SANS Institute Author retains full rights.

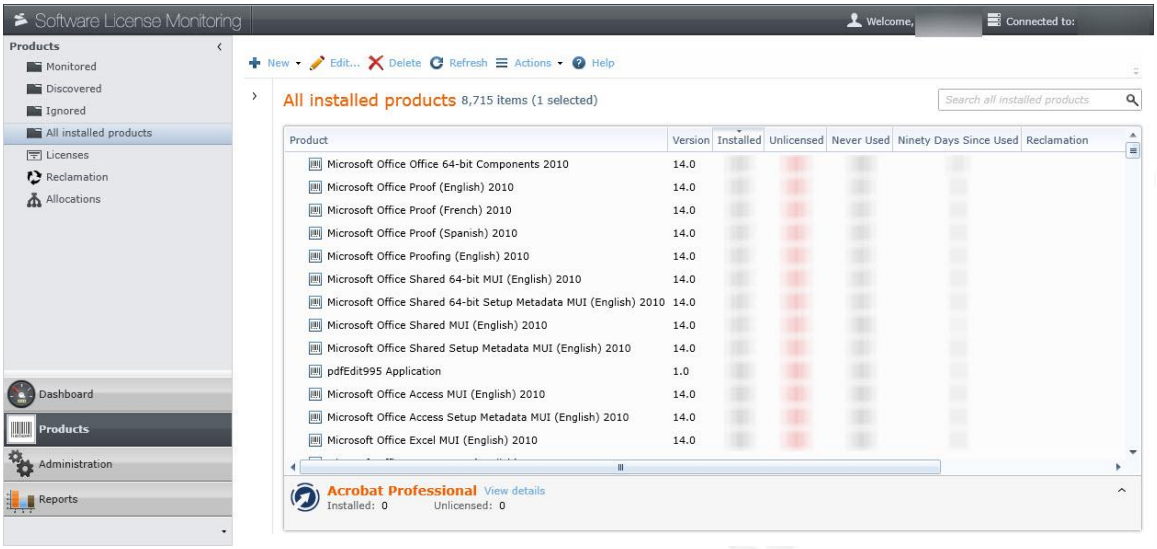


Figure 3: LANDesk SLM Example

The inventory scanner and SLM are tools within LANDesk Management & Security Suite that help IT to fulfill CSC 2 and enhance the business' Cybersecurity program. The information gained about the software can be used to satisfy the CSC 2 System sub-controls 2.1, 2.2, and 2.3 as shown below.

The Center for Internet Security Critical Security Controls Version 6.0 Control Description Critical Security Control #2: Inventory of Authorized and Unauthorized Software		
Family	**Control**	
System	2.1	Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.
System	2.2	Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.
System	2.3	Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. The software inventory systems must be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.
System	2.4	Virtual machines and/or air-gapped systems should be used to isolate and run applications that are required for business operations but based on higher risk should not be installed within a networked environment.

Spreadsheet: 2 CSC-CIS Critical Security Controls VER 6.0 Excel 10.15.2015.xlsx

LANDesk Management and Security Suite has been used for illustrating how a tool can be used to satisfy the company's cybersecurity program. Regardless of the tool chosen, it is more important that the tool satisfies one or more of the requirements of the company's cybersecurity program and as many requirements of the regulations and audits governing the business. In fact, the complexity of the company may make multiple tools, working together, a necessity.

Bob.Mier@agvantis.comRobert.Mier@cox.net

© 2016 The SANS Institute Author retains full rights.

7. Conclusion

Remember, this is not a sprint, cybersecurity is a continuous program that is running 24 hours a day 365 days a year. IT is tasked with protecting and defending the infrastructure of the company while simultaneously enabling the company to be successful and achieve its mission. The Cybersecurity program is the plan that is used in this battle. A mature cybersecurity program takes time to develop and implement. Truthfully, as long as the business is in existence, the cybersecurity program never stops maturing. It must live as the business lives.

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

SunTzu, The Art of War (Sunzi & Cleary, 2005)

For IT to win this Cyberwar, IT has to know the business. To know the business, starts with knowing what endpoints exist within the business. Think CSC 1. IT cannot protect the business if they don't have knowledge of all of the end points (computers, servers, tablets, mobile devices, printers, firewalls, routers, switches, and other network attached devices). Which leads right into knowing what software, think CSC 2, is running on each of these devices. Allowing the authorized software and preventing the unauthorized software from running help the business to be successful. Arming IT to defend the business effectively, IT has to know the business.

With complexity of attacks that IT must battle and with limited resources; the NIST Cybersecurity Framework and Critical Security Controls work together to help the IT staff create an effective defensive "battle plan". The starting point is to be able to see and identify the business end points and the software which is running on them. Once this is known, steps can be taken to evaluate what is authorized and remove what is unauthorized. From there IT can move on to CSC 3 – 20 and continue to utilize the NIST

© 2016 The SANS Institute Author retains full rights.

Cybersecurity Framework to stay focused and on target for defending the business against the ongoing attacks. This is a marathon not a sprint. Just like everything else, you start with what Cybersecurity program you have and then make improvements and enhancements to mature that Cybersecurity Program over time.

©2016 SANS Institute, Author retains full rights.

Bob.Mier@agvantis.comRobert.Mier@cox.net

© 2016 The SANS Institute Author retains full rights.

References

A Measurement Companion to the CIS Critical Security Controls (version 6). (2015, October). Retrieved from HTTPS://www.cisecurity.org/cirtical-controls.cfm

In-text: ("Measurement Companion to the CIS Critical Security Controls (version 6)," 2015)

The Center for Internet Security. (2015). *The CIS Critical Security Controls for Effective Cyber Defense version 6.0*. Retrieved from https://www.cisecurity.org/critical---controls.cfm

This work is licensed under a Creative Commons Attribution--Non Commercial---No Derivatives 4.0 International Public License. The link to the license terms can be found at https://creativecommons.org/licenses/by--nc--nd/4.0/legalcode

In-text: (The Center for Internet Security, 2015, p. xx)

The Center for Internet Security. (2015). *CSC-CIS Critical Security Controls VER 6.0 Excel 10.15.2015.xlsx*. Retrieved from https://www.cisecurity.org/critical---controls.cfm

This work is licensed under a Creative Commons Attribution--Non Commercial---No Derivatives 4.0 International Public License. The link to the license terms can be found at https://creativecommons.org/licenses/by--nc--nd/4.0/legalcode

In-text: (The Center for Internet Security, 2015, Spreadsheet p. 02)

Cybersecurity Framework. (2015, July 8). Retrieved from http://www.nist.gov/cyberframework/ **In-text:** ("Cybersecurity Framework," 2015)

Bob.Mier@agvantis.comRobert.Mier@cox.net

© 2016 The SANS Institute Author retains full rights.

Executive Order -- Improving Critical Infrastructure Cybersecurity | whitehouse.gov. (2013, February 12). Retrieved from https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity In-text: ("Executive Order -- Improving Critical Infrastructure Cybersecurity | whitehouse.gov," 2013)

Identity Theft Resource Center. (2015). *ITRC Breach Stats Report 2015*. Retrieved from http://www.idtheftcenter.org/images/breach/ITRCBreachStatsReport2015.pdf Copyright 2015 Identity Theft Resource Center **In-text:** (Identity Theft Resource Center, 2015, p. xx)

IT Asset Inventory Management | LANDESK. (2016). Retrieved from http://www.landesk.com/products/management-suite/discovery-inventory/ **In-text:** ("IT Asset Inventory Management | LANDESK," 2016)

LANDESK Software, Inc. (2014). *LANDesk Management Suite 9.6 User's Guide*. Retrieved from https://help.landesk.com/Help/download/data/ldms/96/LDMS96Users.pdf **In-text:** (LANDESK Software, Inc, 2014, p. xx)

McCarthy, N. (2014, August 26). Chart: The Biggest Data Breaches in U.S. History. Retrieved from http://www.forbes.com/sites/niallmccarthy/2014/08/26/chart-the-biggest-data-breaches-in-u-s-history/ **In-text:** (McCarthy, 2014)

National Institute of Standards and Technology (U.S.), issuing body. (2014). *Framework for improving critical infrastructure cybersecurity*. Retrieved from http://www.nist.gov/cyberframework/index.cfm **In-text:** (National Institute of Standards and Technology (U.S.), issuing body, 2014, p. xx)

Bob.Mier@agvantis.comRobert.Mier@cox.net

© 2016 The SANS Institute Author retains full rights.

Ponemon Institute. (2015). *2015 Cost of Data Breach Study: Global Analysis*. Retrieved from http://www-03.ibm.com/security/data-breach/index.html **In-text:** (Ponemon Institute, 2015, p. xx)

SANS Institute. (2000). *SANS Institute - CIS Critical Security Controls: A Brief History*. Retrieved December 6, 2015, from https://www.sans.org/critical-security-controls/history **In-text:** (SANS Institute, 2000)

Statista. (2014, August 26). *The Largest Data Breaches in U.S. History* [Graph]. Retrieved from http://www.forbes.com/sites/niallmccarthy/2014/08/26/chart-the-biggest-data-breaches-in-u-s-history/ **In-text:** (Statista, 2014)

Sunzi, & Cleary, T. F. (2005). *The art of war*. Boston, MA: Shambhala. **In-text:** (Sunzi & Cleary, 2005, p. xx)

Bob.Mier@agvantis.comRobert.Mier@cox.net

© 2016 The SANS Institute Author retains full rights.