Interested in learning more about security?

SANS Institute InfoSec Reading Room

Implementing an Information Assurance Awareness Program: A case study for the Twenty Critical Security Controls at Consulting Firm X for IT Personnel

As a consultant within a large, growing, high-profile consulting firm, this challenge is interesting in terms of preventing potential future cyber-attacks. The organization supports a large number of sensitive US Government projects, including hosting or developing portals and applications as part of the work. Protecting this organization s networks indirectly protects sensitive US Government networks as well. Consulting Firm X, known internally as the Firm, primarily supports clients in the public sector and many of...

Implementing an Information Assurance Awareness Program: A case study for the Twenty Critical Security Controls at Consulting Firm X for IT Personnel

GIAC Gold Paper

Author: John Dittmer, jdittmer@suprtek.com

Advisor: Richard Carbone

Accepted: July 15, 2014

Abstract

As a consultant within a large, growing, high-profile consulting firm, this challenge is interesting in terms of preventing potential future cyber-attacks. The organization supports a large number of sensitive US Government projects, including hosting or developing portals and applications as part of the work. Protecting this organization's networks indirectly protects sensitive US Government networks as well. Consulting Firm X, known internally as the Firm, primarily supports clients in the public sector and many of the senior executives are retired senior government and military officials. This relationship has often caused the Firm negative publicity and public opinion among those who do not trust the US Government and its policies. Often, the Firm is the target of cyber-attacks. Therefore, the Firm must maintain a high level of Information Assurance preparedness and awareness in implementing security controls.

1. Introduction

The objective of this paper is to incorporate the lessons of two SANS Technical Institute courses: ISM 6000 (Standards Based Implementation of Security) and ISM 5300 (Building Security Awareness). Often, security incidents are the result of two problems. The first is a lack of standardized security controls. All too frequently, workstations and devices are left unsecured. Thus, there needs to be a method of implementing security controls throughout the organization and its systems. The second is that all too often an organization's personnel, even within its Information Technology (IT) departments, are not knowledgeable on how to secure their systems. An Information Awareness (IA) awareness program often needs to be established within organizations to promote safety and implement new security processes.

2. Background

2.1. Consulting Firm X

Consulting Firm X (CFX or the Firm) is a management and technology-consulting firm based in McLean, Virginia that has been in business since 1914. It was the first management-consulting firm that was not an accounting company first and it primarily supported commercial clients until World War II. [1] During the war, the Firm restructured itself as a provider of technology and engineering services. In fact, CFX's reputation grew to the point that the Navy directly commissioned some of its senior managers as Navy Captains so they could directly oversee special engineering projects. [1] After World War II, the Firm's attention grew to support United States (US) Federal government clients, especially in the US Department of Defense (DoD) and the Intelligence Community (IC). [1] In time, many senior government executives and retired military officers became senior executives and partners with the Firm, which has helped CFX win continued business from the Federal government.

Since CFX's senior management enjoys long-standing relationships with many senior government and military officials, politically liberal groups and press often scrutinize the activities of the Firm. In fact, Bloomberg BusinessWeek has dubbed CFX as the "World's Most Profitable Spy Organization". [2] The recent scandal involving Edward Snowden and intelligence leaks associated with the Firm have made hack activists and others who wish to discredit the Firm try to break into its information systems. In addition, as a major Federal

contractor, there is always the concern that hackers and foreign intelligence operatives may want to use CFX's networks as a backdoor means to break into government networks since there are many connections with government networks. An example of such activity was Operation Aurora in which major defense firms such as Lockheed Martin were allegedly attacked by Chinese-based hackers in 2009. Other firms that were affected by the attacks included Adobe and Google. [3] In addition, CFX operates government activities such as web sites and portals, so attacks on them are a distinct possibility, especially since they can lead to infiltrating sensitive government networks.

In terms of infrastructure scale, CFX's networks support over 26,000 employees plus contractors. These employees are located in thirty US states, plus Afghanistan, Germany, Japan, Kazakhstan, Saudi Arabia, South Korea, United Arab Emirates and the United Kingdom.

2.2. CFX's Participation in the Defense Industrial Base (DIB) Cyber Security / Information Assurance Program

Because of its high profile and continued threats against its infrastructure, CFX participates in the DoD Defense Industrial Base (DIB) Cyber Security/Information Assurance (IA/CS) Program. The program is described by its web site as "a voluntary program to enhance and supplement DIB participants' capabilities to safeguard DoD information that resides on or transits, DIB unclassified information systems". [4] The intention of the program is to prevent a contractor's networks from becoming the backdoor for cyber-attacks on networks of DoD and other defense contractors. The program is based on voluntary participation.

By participating in the program, CFX receives unclassified cyber threat indicators and related, classified contextual information. DIB companies can choose whether to incorporate the indicators into their own traffic screening or other security tools and they can use the contextual information to better understand and defend against the cyber security threats they face. DoD also shares mitigation measures to assist DIB Companies' cyber security efforts. DIB companies also report known intrusion events to the Government and may participate in Government damage assessments, if needed. A DIB company may report any cyber security event that may be of interest to the to the Government and DIB cyber community, at its discretion.

As an additional and optional part of the program, the Government will furnish classified threat and technical information to participating DIB Companies or their Commercial Service Providers (CSPs), on a voluntary basis. This sensitive Government furnished information enables DIB companies or CSPs on behalf of their DIB customers, to counter additional types of known malicious activity and to further protect DoD program information. [4]

While information sharing about malicious activities among defense contractors and their Federal clients is a great start, it is by no means a total solution. Companies, government agencies and other large organizations need a method of implementing security controls on their own IT infrastructure. One such method is the Twenty Critical Controls.

2.3 Historical Background

The Twenty Critical Security Controls for Effective Cyber Defense (CSC is also known as the Consensus Audit Guidelines or CAG) is a publication of best practice guidelines for information assurance. The initiative to create the controls was initiated early in 2008 as a response to extreme data losses experienced by organizations in the US Defense Industrial Base.

In response to a request from the White House staff in 2008, the Office of the Secretary of Defense asked the National Security Agency (NSA) for help setting priorities for the myriad security controls that were available for cybersecurity. [5] Since budgets and resources for cybersecurity initiatives were limited, priorities for security controls had to be set. The request was sent to NSA because that agency had the best reputation for understanding how cyber-attacks were carried out and which were most commonly used. The request came at a moment when the theme "offense must inform defense" had become the primary philosophy for cybersecurity within the Bush Administration. [5]

The objective was to help DoD prioritize its cybersecurity spending and maximize use of its resources. NSA had been refining a list of security controls that were most effective in stopping known attacks since the early 2000s based on previous requests from the military services, reinforced by guidance from the White House. Many of these security controls were derived from assessing common vulnerabilities that appeared during NSA Red Team exercises. Tom Donahue, an employee of the Central Intelligence Agency, who was assigned to the White

House cyber policy team at the time, described the mandate as follows: "first fix the known bads". [5] This guidance meant no security control should be made a priority unless it could be shown to stop or mitigate a known attack. That mandate was the key that came to separate the 20 Critical Controls from most other lists of controls. [5]

The list of key controls that blocked the most frequent attacks was designated "For Official Use Only" (FOUO) and could not be widely shared because the designation meant that the information, although unclassified, was still restricted from public disclosure, including sharing with non-government entities. Fortunately, NSA had already been participating in a public-private partnership involving the Center for Internet Security (CIS) and the SANS Institute for more than a decade. When John Gilligan of CIS and Alan Paller of SANS approached the NSA leadership, it agreed to participate in a public-private consortium to share its attack information. The consensus of all three organizations was that NSA should provide the same type of control-prioritization knowledge for civilian government agencies and critical infrastructure. NSA agreed on the basis that the military could not protect the United States and its vital interests if the nation's critical communications, power and financial sectors were not protected. [5]

The consortium members were expanded to include additional organizations that had formal access to high value threat information, either because they had large teams that developed and used attack techniques or because they had large teams that performed the deep after-attack analysis that disclosed tactics, techniques and method used by attackers. [5] Additions to the coalition included the British government's Communications-Electronics Security Group (CESG) and Centre for the Protection of National Infrastructure (CPNI), the DoD Computer Network Defense Architect (who had previously led the NSA Red Teams before moving to DoD Chief Information Officer) staff and the Federal Bureau of Investigations Intelligence Community – Joint Task Force (IC-JTF). [5][6][7] In addition, a number of companies in the incident response field, such as Mandiant and InGuardians, who did high value analysis of major attacks, were included. Further expansion brought in the Defense Cyber Crime Center, three DOE laboratories and companies including McAfee and Lockheed Martin, which had experience in responding to major breaches. [5]

As the group developed the security controls, it built consensus at each step. Many observers within the cybersecurity community were surprised by the willingness of many companies and organizations to share sensitive cyber-attack information. Two overarching factors enabled this active sharing. First, there was the agreement that only actual attack information could be used to justify adding any controls so as not to create an undue burden to participating organizations. [5] Second, the consortium's membership was so impressive that participants knew that the results would be authoritative. [5] They wanted to be active contributors to something that could make a difference in protecting the national information infrastructure. [5] Surprisingly, the clear consensus of the consortium was that the 20 Critical Controls addressed the most prevalent attacks found in government and industry. However, this consensus goes along the lines of a concept in management theory known as the Pareto Principle (also known as the 80–20 Rule, the Law of the Vital Few and the Principle of Factor Sparsity). This concept states that, for many events, roughly 80% of the effects come from 20% of the causes. [8]

This development became the focus for an initial draft document. An initial draft of the 20 Critical Controls was circulated in early 2009 to several hundred information technology and security organizations for further review and comment. Over 50 organizations commented on the draft. They overwhelmingly endorsed the concept of a focused set of controls and the selection of the 20 Critical Controls. According to CSIS, these 50 organizations also provided valuable "fine-tuning" to the descriptions of the controls. The consortium reconnected with current and additional members every 6 to 12 months to ensure new attack information was fully reflected and that new techniques for mitigating old attacks were included. Other improvements to the 20 Critical Controls over time included measures by which organizations could know how well they had implemented the controls and a list of automated tools that have been validated (by thorough reference checks) to be effective in implementing the controls. [5]

During the fall of 2008, the Center for Strategic and International Studies (CSIS) had convened a bipartisan panel, at the request of two leading members of Congress, which was called the Commission on Cybersecurity for the 44th Presidency. As a continuation of the Commission's work, it was natural for CSIS to become the first publisher of the 20 Critical Controls. [5]

Following up the publication of the 20 Critical Controls, the U.S. Department of State validated the consensus controls in 2009 by determining whether the controls covered the 3,085 attacks it had experienced in Fiscal Year 2009 (the period between 10/01/2008 – 09/30/2009). [5] In a presentation to the Intelligence Community, the State Department's Chief Information Security Officer (CISO), John Streufert, reported remarkable alignment between the consensus controls and the actual attacks experienced by the State Department. [9] He also launched a program to implement automated capabilities to enforce the key controls and provide daily mitigation status information to every system administrator across 24 time zones in which the State Department operates. [9] This marked the beginning of the movement towards Continuous Monitoring within the US Federal Government rather than relying on periodic certification and accreditation (C&A) processes; these processes provide a snapshot of the status of information security at a point in time. Having rapidly achieved a reduction of more than 88% in vulnerability-based risk across 85,000 systems, the State Department's program became a model for large government and private sector organizations. [9] In December of 2011, then Secretary of Homeland Security Janet Napolitano appointed John Streufert as the Director of the National Cybersecurity Division, with the mandate to bring about the same type and level of risk reduction across the government and its critical infrastructure as he had done at the State Department. [9]

Also in December 2011, the United Kingdom's Centre for the Protection of National Infrastructure (CPNI) announced to British government agencies and critical industries that their government would adopt the 20 Critical Controls as the framework for securing their critical infrastructure going forward. [7] Moreover, as of May 2012, the Commander of the US Cyber Command and Director of NSA at the time, General Keith Alexander, announced that he believed the adoption of the 20 Critical Controls was a good foundation for effective cybersecurity. In addition, he stated that they are an excellent example of how public and private sector organizations can voluntarily come together to improve security. His endorsement was the result of NSA's investment over the period of a year with some of its top talent vetting the 20 Critical Controls to be certain they reflected the actual risks faced by industrial and government systems. [5]

In June 2012, the Idaho National Laboratory, home of the U.S. Department of Energy's National SCADA Test Bed, completed a very favorable analysis of how the 20 Critical Controls applied to the electric sector as a first step in assessing the applicability of various controls specific to industrial sectors. [5]

To continue the work of sustaining the 20 Critical Controls and to encourage broad adoption and implementation globally, the stewardship of the Controls was transferred to the Council on Cybersecurity in 2013. As an independent, global non-profit entity, the Council engages broad communities of stakeholders to identify, validate, promote and sustain cybersecurity best practices, chief among them being the 20 Critical Controls. [5]

3. Listing of the 20 Critical Security Controls

As this paper discusses how to implement the 20 Critical Security Controls, it is time to describe them. The description will only be a summary since others could easily write a lengthy document describing them in detail. For the purposes of this discussion, Version 5 of the controls will be described in the subsequent listing:

3.1 Critical Security Control #1: Inventory of Authorized and Unauthorized Hardware Devices

- Description: Actively manage (inventory, track and correct) all hardware devices on the network so that only authorized devices are given access and both unauthorized and unmanaged devices are found and prevented from gaining access. [10]
- Why is it critical?: Often devices, especially laptops, come and go off an enterprise's network and so they get out of synch with required patches and security updates thereby making them susceptible to attacks. In addition, hackers can take advantage of new hardware that is installed on the network one evening but not configured and patched with appropriate security updates until the following day. Intruders may already have gained internal access and when searching for internal jump points or victims they can use these insecure devices. Additional systems connected to the enterprise's network such as demonstration systems, temporary test systems and guest networks should be managed carefully and/or isolated in order to prevent adversarial access from affecting the security of enterprise operations. As

new mobile technology continues to come out, the BYOD (bring your own device) trend where employees bring personal devices into work and connect them to the network is becoming very common. These devices could already be compromised and be used to infect internal resources. [10]

- Comments: Managed control of all devices also plays a critical role in planning and executing system backup and recovery. [10]

3.2 Critical Security Control #2: Inventory of Authorized and Unauthorized Software

- Description: Actively manage (inventory, track and correct) all software on the network so that only authorized software is installed and can execute such that unauthorized and unmanaged software are found and prevented from installation or execution. [10]
- Why is it critical?: Targeted organizations such as CFX are continuously scanned by hackers for vulnerable versions of software that can be remotely exploited. Some attackers also distribute hostile web pages, document files, media files and other content via their own web pages or otherwise trustworthy third-party sites. When unsuspecting victims access this content with a vulnerable browser or other client-side program, attackers compromise their machines, often installing backdoor programs and bots that give the attacker long-term control of the system. Some sophisticated attackers may use zero-day exploits, which take advantage of previously unknown vulnerabilities for which no patch has yet been released by the software vendor. Without proper knowledge or control of the software deployed in an organization, defenders cannot properly secure their assets. [10]

Poorly controlled machines are more likely to be either running software that is not needed for business purposes, introducing potential security flaws or running malware introduced by an attacker-compromised system. Once a single device has been exploited, attackers often use it as a staging point for collecting sensitive information. In addition, compromised machines are used as a launching point for movement throughout the network and collaborating networks. In this way, attackers may quickly turn one compromised machine into many. Organizations that do not have complete software inventories are unable to find

systems running vulnerable or malicious software so as to mitigate problems or root out attackers. [10]

- Comments: Managed control of all software also plays a critical role in planning and executing system backup and recovery. [10]

3.3 Critical Security Control #3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

- Description: Establish, implement and actively manage (track, report on, correct) the security configuration of laptops, servers and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. [10]
- Why is it critical?: Default configurations for operating systems and applications are normally geared towards ease-of-deployment and ease-of-use – not security as they are delivered. Basic controls, open services and ports, default accounts or passwords, older (vulnerable) protocols, pre-installation of unneeded software; many can be exploited in their default state. [10]
- Comments: Developing configuration settings with appropriate security properties is a complex task beyond the ability of individual users, requiring analysis of potentially hundreds or thousands of options in order to make good choices. Even if a strong initial configuration is developed and installed, it must be continually managed to avoid security "decay" as software is updated or patched, new security vulnerabilities are reported and configurations are "tweaked" to allow the installation of new software or support new operational requirements. If not, attackers will find opportunities to exploit both network-accessible services and client software. [10]

3.4 Critical Security Control #4: Continuous Vulnerability Assessment and Remediation

- Description: Continuously acquire, assess and take action on new information in order to identify vulnerabilities, remediate and minimize the window of opportunity for attackers. [10]
- Why is it critical?: Cyber defenders must operate in a constant stream of new information: software updates, patches, security advisories, threat bulletins, etc. Understanding and managing vulnerabilities has become a continuous activity, requiring significant time, attention and resources. [10]

  Attackers can get access to the same information and they can take advantage of gaps between the appearance of new knowledge and remediation. For instance, when researchers report new vulnerabilities, a race starts among all parties, including attackers (to "weaponize", deploy an attack, exploit), vendors (to develop, deploy patches or signatures and updates) and defenders (to assess risk, regression-test patches, install). [10]
- Comments: Organizations that do not scan for vulnerabilities and proactively address discovered flaws face an increased possibility of having their computer systems compromised. Defenders face particular challenges in scaling remediation across an entire enterprise and prioritizing actions with conflicting priorities including sometimes-uncertain side effects. [10]

3.5 Critical Security Control #5: Malware Defenses

- Description: Control the installation, spread and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering and corrective action. [10]
- Why is it critical?: Malicious software is an integral and dangerous aspect of Internet threats, which may have been designed to attack systems, devices or data. It can be fast moving, fast changing and enter through any number of points including end-user devices, e-mail attachments, web pages, cloud services, user actions and removable media. Modern malware can be designed to avoid defenses, to attack or even disable them. [10]
- Comments: Malware defenses must be able to operate in this dynamic environment through large-scale automation, rapid updating and integration with processes like Incident Response. They must also be deployed at all possible points-of-attack in order to detect, stop and control the movement and execution of malicious software. Enterprise endpoint security

suites provide administrative features to verify that all defenses are active and current on every managed system. [10]

3.6 Critical Security Control #6: Application Software Security

- Description: Manage the security lifecycle of all in-house developed and acquired software in order to prevent, detect and correct security weaknesses. [10]
- Why is it critical?: Often, vulnerabilities found in web-based and other application software. They are present for many reasons, including coding mistakes, logic errors, incomplete requirements and failure to test for unusual or unexpected conditions. [10]
- Comments: There is a wealth of information about such vulnerabilities available to attackers and defenders alike, as well as a robust marketplace for tools and techniques to allow for the "weaponization" of vulnerabilities into exploits. Attackers can inject specific exploits, including buffer overflows, SQL injection attacks, cross-site scripting, cross-site request forgery and click jacking of code to gain control over vulnerable machines. [10]

3.7 Critical Security Control #7: Wireless Access Control

- Description: The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LAN), access points and wireless client systems. [10]
- Why is it critical?: Major data thefts have been initiated by attackers who have gained wireless access to organizations from outside the physical building, bypassing organizations' security perimeters by connecting wirelessly to access points inside the organization. Wireless clients accompanying traveling officials are infected on a regular basis through remote exploitation during air travel or in cyber cafés. Such exploited systems are then used as back doors when they are reconnected to the network of a target organization. Still other organizations have reported the discovery of unauthorized wireless access points on their networks, planted and sometimes hidden for unrestricted access to an internal network. [10]
- Comments: Wireless devices are a convenient vector for attackers to maintain long-term access into a target environment. [10]

3.8 Critical Security Control #8: Data Recovery Capability

- Description: The processes and tools used to back-up critical information properly with a proven methodology for its timely recovery. [10]
- Why is it critical?: When hackers compromise machines, they often make significant changes to configurations and software. Sometimes, subtle alterations of data stored on compromised machines are made, potentially jeopardizing organizational effectiveness with polluted information. [10]
- Comments: When attacks are discovered, it can be very difficult for organizations without a trustworthy data recovery capability to remove all aspects of the attacker's presence on a machine. [10]

3.9 Critical Security Control #9: Security Skills Assessment and Appropriate Training to Fill Gaps

- Description: Identifying the specific knowledge, skills and abilities needed to support the defense of the enterprise for all functional roles in the organization (prioritizing those mission-critical to the business and its security). Also, developing and executing an integrated plan to assess, identify gaps and remediate through policy, organizational planning, training and awareness programs. [10]
- Why is it critical?: At every stage of system design, implementation, operation, use and oversight, people fulfill important functions. Examples include the actions of end-users (who can fall prey to social engineering schemes such as phishing), IT operations (who may not recognize the security implications of IT artifacts and logs), security analysts (who struggle to keep up with an explosion of new information) and system developers (who don't understand the opportunity to resolve root cause vulnerabilities early in the system life-cycle). In addition, this includes executives and system owners (who struggle to quantify the role that cybersecurity plays in overall operational/mission risk). [10]
- Comments: Training users about good cyber defense habits has been proven to increase readiness and prevent incidents. [10]

3.10 Critical Security Control #10: Short Title: Secure Configurations for Network Devices such as Firewalls, Routers and Switches

- Description: Establish, implement and actively manage (track, report on, correct) the security configuration of network infrastructure devices using rigorous configuration

management and change control processes in order to prevent attackers from exploiting vulnerable services and settings. [10]

- Why is it critical?: The default configurations for network infrastructure devices are geared towards ease-of-deployment and ease-of-use, not security. Open services and ports, default accounts (including service accounts) or passwords, support for older (vulnerable) protocols and pre-installation of unneeded software may be exploitable in their default state. Hackers take advantage of network devices becoming less securely configured over time as users demand exceptions for specific business needs. [10]
- Comments: By closing the gaps in security configurations, many security incidents can be prevented in the first place since intruders tend to follow the path of least resistance. [10]

3.11 Critical Security Control #11: Limitation and Control of Network Ports, Protocols and Services

- Description: Manage (track/control/correct) the ongoing operational use of ports, protocols and services on networked devices in order to minimize windows of vulnerability available to attackers. [10]
- Why is it critical?: Attackers search for remotely accessible network services that are vulnerable to exploitation. Common examples include poorly configured web servers, mail servers, file and print services and Domain Name Service (DNS) servers installed by default on a variety of device types, often without a business need for the given service. Many software packages automatically install services and turn them on as part of their installation without informing the user or administrator that the services have been enabled. Attackers scan for such issues and attempt to exploit these services, often attempting default user IDs and passwords or widely available exploitation code. [10]
- Comments: Organizations should have their IT Departments institute processes to carefully monitor and manage their systems' ports, protocols and services. [10]

3.12 Critical Security Control #12: Controlled Use of Administrative Privileges

- Description: The processes and tools used to track/control/prevent/correct the use, assignment and configuration of administrative privileges on computers, networks and applications. [10]
- Why is it critical?: The misuse of administrative privileges is a primary method for attackers to spread inside a target enterprise. Two very common attacker techniques take advantage of uncontrolled administrative privileges. In the first, a workstation user running as a privileged user is fooled into opening a malicious e-mail attachment, downloading and opening a file from a malicious website or simply surfing to a website hosting attacker content that can automatically exploit browsers. The second common technique used by attackers is an elevation of privileges by guessing or cracking a password for an administrative user in order to gain access to a target system. If administrative privileges are loosely and widely distributed or identical to passwords used on less critical systems, the attacker has a much easier time gaining full control of systems, because there are many more accounts that can act as avenues for the attacker to compromise administrative privileges. [10]
- Comments: IT Departments need to minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative or privileged functions and monitor for anomalous behavior. They should also use automated tools to conduct an inventory of all administrative accounts and validate the authorization of their privileges. [10]

3.13 Critical Security Control #13: Boundary Defense

- Description: Organizations need to detect, prevent and correct the flow of information transferring between networks of different trust levels with a focus on security-damaging data. [10]
- Why is it critical?: Attackers focus on exploiting systems that they can use to reach across the Internet, including not only De-Militarized Zone (DMZ) systems but also workstation and laptop computers that pull content from the Internet through network boundaries. Threats such as organized crime groups and nation-states use configuration and architectural weaknesses found on perimeter systems, network devices and Internet-accessing client systems in order to gain initial access into an organization. Then, with a base of operations established from these systems, attackers can pivot to get deeper inside the boundary to steal

or change information or to set up a persistent presence for future attacks against internal hosts. Additionally, many attacks occur between business partner networks, sometimes referred to as extranets, as attackers hop from one organization's network to another, exploiting vulnerable systems on extranet perimeters. [10]

- Comments: To control the flow of traffic through network borders, police content by looking for attacks and evidence of compromised machines. Boundary defenses should be multi-layered, relying on firewalls, proxies, DMZ perimeter networks and network-based IPS and IDS systems. It is also critical to filter both inbound and outbound traffic. [10]

3.14 Critical Security Control #14: Maintenance, Monitoring and Analysis of Audit Logs

- Description: Collect, manage and analyze audit logs of events that could help detect, understand or recover from an attack. [10]
- Why is it critical?: Deficiencies in security logging and analysis allow attackers to hide their location, malicious software and activities on victim machines. Sometimes, logging records are the only evidence of a successful attack. Even if the victims know that their systems have been compromised, without protected and complete logging records, they are blind to the details of the attack and to subsequent actions taken by the attackers. Without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible. [10]
- Comments: Countermeasures include establishing at least two synchronized time sources (i.e., Network Time Protocol - NTP) from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent and are set to UTC (Coordinate Universal Time). In addition, IT Departments should validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses and various other useful elements of each packet and/or transaction. [10]
-

3.15 Critical Security Control #15: Controlled access based on the Need to Know

- Description: The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources and systems) according to the formal determination of which persons, computers and applications have a need and right to access these critical assets based on an approved classification. [10]
- Why is it critical?: Some organizations do not carefully identify and separate their most sensitive and critical assets from less sensitive, publicly accessible information on their internal networks. In many environments, internal users have access to all or most of the critical assets. Sensitive assets may also include systems that provide management and control of physical systems (e.g., SCADA). Once attackers have penetrated such a network, they can easily find and exfiltrate important information, cause physical damage or disrupt operations with little resistance. For example, in several high-profile breaches over the past two years, attackers were able to gain access to sensitive data stored on the same servers with the same level of access as far less important data. There are also examples of using this type of attack to gain access to the corporate network and then control over physical assets and cause damage. [10]
- Comments: This is a long-established practice in the US military and intelligence communities. However, different organizations need to establish their own policies, especially in light of new laws and policies regarding privacy. [10]

3.16 Critical Security Control #16: Account Monitoring and Control

- Description: Actively manage the life cycle of system and application accounts – their creation, use, dormancy and deletion in order to minimize opportunities for attackers to leverage them. [10]
- Why is it critical?: Attackers frequently discover and exploit legitimate but inactive user accounts in order to impersonate legitimate users, thereby making discovery of attacker behavior difficult for network watchers. Accounts for contractors and employees who have been terminated and accounts formerly set up for Red Team testing (but not deleted afterwards) have often been misused in this way. Additionally, some malicious insiders or former employees have accessed accounts left behind on a system long after contract expiration, maintaining their access to an organization's computing system and sensitive data for unauthorized and sometimes malicious purposes. [10]

- Comments: All system accounts should be reviewed. Any account not associated with a legitimate business process and owner should be disabled. All accounts should have an associated expiration date and be regularly monitored. [10]

3.17 Critical Security Control #17: Data Protection

- Description: The processes and tools used to prevent data exfiltration can be used to mitigate the effects of exfiltrated data and ensure the privacy and integrity of sensitive information. [10]
- Why is it critical?: Data resides in many places. Protection of that data is best achieved through the application of a combination of encryption, integrity protection and data loss prevention techniques. As organizations continue their move towards cloud computing and mobile access, it is important that proper care be taken to limit and report on data exfiltration while also mitigating the effects of data compromise. [10]
- Comments: The adoption of data encryption, both in transit and at rest, provides mitigation against data compromise. This is true if proper care has been taken in the processes and technologies associated with encryption operations. An example of this is the management of cryptographic keys used by the various algorithms that protect data. [10]

3.18 Critical Security Control #18: Incident Response and Management

- Description: Protect the organization's information, as well as its reputation by developing and implementing an incident response infrastructure (e.g. plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence and restoring the integrity of the network and systems. [10]
- Why is it critical?: Cyber incidents are now just part of our way of life. Even large, well-funded and technically sophisticated enterprises struggle to keep up with the frequency and complexity of attacks. The question of a successful cyber-attack against an enterprise is not "if" but "when". When such an incident occurs, it is too late to develop the right procedures, reporting, data collection, management responsibility, legal protocols and communications strategy that will allow the enterprise to successfully understand, manage and recover during

incidents. Without an incident response plan, an organization may not discover an attack in the first place, or, if the attack is detected, the organization may not follow good procedures to contain damage, eradicate the attacker's presence and recover in a secure fashion. Thus, the attacker may have a far greater impact, causing more damage, infecting more systems and possibly exfiltrate more sensitive data than would otherwise be possible were an effective incident response plan in place. [10]

- Comments: Ensure that there are written incident response procedures that include a definition of personnel roles for handling incidents. The procedures should define the phases of incident handling. Define management personnel who will support the incident handling process by acting in key decision-making roles. Conduct periodic incident scenario sessions for personnel associated with the incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the incident handling team. [10]

3.19 Critical Security Control #19: Secure Network Engineering

- Description: Make security an inherent attribute of the enterprise by specifying, designing and building-in features that allow high confidence systems operations while denying or minimizing opportunities for attackers. [10]
- Why is it critical?: System or security designers rarely get to start from scratch and build in all of the security features they might want. In addition, even if they did, systems constantly evolve, new business imperatives appear, attackers develop new techniques and new technologies emerge to complicate the security problem. In such an environment, attackers take advantage of missing security features, time gaps in deploying new defenses or moving information and the "seams" between defensive controls. [10]
- Comments: Design the network using a minimum of a three-tier architecture (DMZ, middleware and private network). Any system accessible from the Internet should be on the DMZ but they should never contain sensitive data. Any system with sensitive data should reside on the private network and never be directly accessible from the Internet. DMZ systems should communicate with private network systems through an application proxy residing on the middleware tier. In addition, segment the enterprise network into multiple,

separate trust zones to provide a more granular control of system access and additional intranet boundary defenses. [10]

3.20 Critical Security Control #20: Penetration Tests and Red Team Exercises

- Description: Test the overall strength of an organization's defenses (the technology, the processes and the people) by simulating the objectives and actions of an attacker. [10]
- Why is it critical?: Attackers often exploit the gap between good defensive designs and intentions and implementation or maintenance. Examples include the time window between announcement of a vulnerability, the availability of a vendor patch and actual installation on every machine; well-intentioned policies which have no enforcement mechanism; failure to apply good configurations and other practices to the entire enterprise or to machines that come in-and-out of the network. Other examples include failure to understand the interaction among multiple defensive tools or with normal system operations that have security implications. [10]

  In addition, successful defense requires a comprehensive program of technical defenses, good policy and governance and appropriate action by people. In a complex environment where technology is constantly evolving and new attacker tradecraft appears regularly, organizations should periodically test their defenses to identify gaps and to assess their readiness. [10]

  Penetration testing starts from the identification and assessment of vulnerabilities that can be identified in the enterprise. It complements this by designing and executing tests that demonstrate specifically how an adversary can either subvert the organization's security goals (e.g., the protection of specific Intellectual Property) or achieve specific adversarial objectives (e.g., establishment of a covert Command and Control infrastructure). The result provides deeper insight, through demonstration, into the business risks of various vulnerabilities. [10]
- Comments: Red Team exercises take a comprehensive approach to the full spectrum of organizational policies, processes and defenses in order to improve organizational readiness, improve training for defensive practitioners and inspect current performance levels.

Independent Red Teams can provide valuable and objective insights about the existence of vulnerabilities and the efficacy of defenses and mitigating controls already in place and even for those planned in future implementations. [10]

3.21 Benefits of Implementing the 20 Critical Security Controls

There are several benefits to implementing the 20 Critical Security Controls. According to an article in *SecurityWeek* magazine in 2013 [11], a survey conducted by the SANS Institute of CIOs, system administrators and compliance auditors had the following results. First, eighty percent of the respondents stated they believe that adopting these controls would help them manage vulnerability and improve risk posture. Second, eighty percent of those who have already implemented the controls believed that they have already reduced risk. Third, forty-seven percent of participants have reassessed replacing older technologies, thus perhaps saving money that they might have otherwise spent. Finally, forty-three percent of those who answered said that they have identified security gaps and are purchasing the appropriate new technology to fill in these gaps. [11]

In addition to improving the security posture and reducing risk through technical means, security personnel are identifying security solutions that do not require a change in technology or added costs. For example, the recent Data Breach Investigations Report from Verizon (DBIR) determined that 97 percent of breaches could have been prevented if the default and weak passwords had been changed. [11][12] Moreover, many organizations give end-users administrative privileges (generally an unnecessary risk) and are often running outdated software. Another benefit is reducing the cost for organizations in terms of paying fines and fees for non-compliance. For example, medical groups in the United States are often fined for violations of the Health Insurance Portability and Accountability Act of 1996 (known as HIPPA) because that law is designed to protect patient's sensitive health-related information from being comprised. In the United States, there is a standard among the major credit card companies called the Payment Card Industry Data Security Standard (PCI DSS). It applies to all companies and organizations that process credit, debit and charge cards. Companies and organizations which fail to meet the standard after security assessments and scanning are required to pay fines and undergo further security assessments until they meet the standard. The 20 Critical Security

Controls have been proven to reduce these costs by helping organizations pass the assessments and scan the first time. [11]

In a SANS white paper by Jim D. Hietala, *Implementing the Critical Security Controls*, two real world implementations of the 20 Critical Controls (he refers to them as the Critical Security Controls or CSCs) were examined in detail as case studies. [13] The first case study was the implementation of controls for the city government of Portland, Oregon. The case study described the existing conditions, how the implementation team chose which controls to implement first and then the implementation process itself.

Hietala reported the team's work included various benefits. First, the security team saw fewer hits or incidents of endpoints being infected, a visible indicator that security was improving for the city. The team leader attributed this development to the progress made across the city government in limiting administrative privileges and making frequency and coverage improvements in patching. Another indicator of improvement comes in the form of fewer trouble tickets being issued for configuration issues. The city now uses standardized images for desktops and servers and ensures policy conformance through the directory service. Although this result may not be a direct benefit to security, it helps the IT organization focus on higher-value tasks, such as improving the security posture that demonstrates to the user community that security and stability go together. [13]

Along these lines, the biggest benefits the team leader found while adopting the CSCs came in the form of additional structure for the information security program and a framework for planning additional projects and measuring their progress. A more subtle benefit of adopting the CSCs is the acceptance of a common vocabulary throughout the IT organization, as seen once again in the adoption of Active Directory group policies. Before the team began its work, Group Policy was not commonly used in the city's IT environment, but by using it to implement the CSCs, IT staff members now grasp the feature's benefits. [13]

Finally, as the security vocabulary and controls were accepted, the city government's operations and business groups became more receptive to embracing security enhancements. The IT staff now understands the goals of each of the CSCs and how they will improve security when adopted. [13]

In the second case study, Hietala examined the situation at Spanish financial institution, Bankia. The bank was created in 2011 as the result of the merger of seven Spanish banks. A couple of the banks that were merged had already started information security initiatives. However, it was decided that instead of imposing a new infrastructure, the new bank would establish common processes and terminology [13].

The bank's leaders decided to use the Critical Security Controls for the following purposes. First, they used the CSCs in establishing goals and objectives. Second, the CSCs helped IT staff measure activities and their results, thus helping to track progress in implementing better security. Third, the bank's managers used the CSCs to define criteria success. Finally, the IT staff followed the CSCs recommendations in managing frequent vulnerability scanning and remediation toward continuous improvement. [13]

The result of incorporating the controls into its process proved beneficial to Bankia. For example, significantly more vulnerabilities were discovered and fixed. Checks on web applications are now happening more frequently. Staff hours for manually scanning applications were significantly reduced and the cost of mitigating vulnerabilities was reduced as well. The repair of vulnerabilities was streamlined while cost and overhead resources required for managing web applications were reduced significantly. As more applications were being repaired, the likelihood of a security comprise was reduced. In conclusion, Bankia used the 20 Critical Controls to conduct a successful merger of the networks and applications of the seven banks while improving security. [13]

4. Establishing an Information Security Awareness Program

4.1 The Purpose of Having an IA Awareness Program for Technical Staff

Implementing the Critical Security Controls can be successfully used to improve the level of information protection for an organization such as CFX, it is necessary to examine the methods for doing so. As quoted in the SANS "Securing the Human" Brochure, most organizations have already invested heavily in technical security solutions. [14] However, these solutions will not protect the organizations' information if their people (e.g. end-users, security

staff, IT personnel, senior management, etc.) fail to apply the technical solutions properly or fail to use safe security practices. [14] For example, an organization giving every end-user administrative privileges lends itself to security risks since most users are not trained to properly configure their devices. Another example is when an organization has its system administrators using the same password across all their network devices.

Thus, in order to implement the Critical Security Controls, organizations need to make their personnel aware of proper IA practices and develop an IA Awareness Program. For the purposes of this paper, the author uses CFX as an example of how to create such a program among its IT personnel since the firm is a large, international enterprise that has multiple sites and is a frequent target of hackers and hack-activists.

4.2 Factors to Consider in the Development of the IA Awareness Program

In the development of the IA Awareness Program, the project charter for establishing the steering committee or working group that will develop the program needs to keep the following principles in mind [14]:

- Policies tell users what to do;
- Training provides users with the skills to perform it;
- Awareness changes their behavior.

As part of developing Information Assurance Awareness Program for an international organization as large and diverse as CFX, it is necessary to account for the following factors:

- Culture/Diversity: CFX, as a major consulting firm, tends to act very traditionally. It has a formal command structure and hierarchy while stressing formal processes for most of its activities. In many ways, it tends to act more like a legal or accounting firm than a technology firm does. Part of this formality is that its leadership is very concerned about the legal liability of its activities. Meanwhile, the Firm also stresses diversity in its hiring and human resources practices. Therefore, CFX has to account for language differences, accents, cultural norms, etc., while developing training materials. A couple of methods to achieve this goal is to include stakeholders or members within the steering committee or working group that can help review content to ensure it is 'neutral' or non-offending in

nature. In addition, the communications, human resources or diversity departments can be used to provide expert advice on developing effective programs without creating issues over inappropriate content.

- Language: In addition to culture issues, CFX needs to account for language issues. Although most of the technical staff frequently speaks English, the language has various dialects and slang, dependent on location. Again, the same resources listed above for cultural issues can be reused.
- Imagery: CFX has specific corporate policies regarding the use of corporate images and those from the Internet. It does not permit simply copying images from the web, even if they are free or public domain. The Firm is concerned about liability and copyright infringement, so the legal and communications departments must be consulted. The communications department can help with this activity.
- Training processes: The Firm has several in-house training teams and contractor trainers, along with a training portal with an extensive range of courses. Therefore, CFX needs to leverage its training teams and vendors to help develop and deliver training while showing technical staff what resources are available for follow-on training such as how to secure specific operating systems or applications. Since all of these resources require funding, an extensive and detailed budget should be developed for senior level approval in the earliest stages. [15]
- Establishing IA Workforce Training & Certification requirements: Too often, IA personnel are given roles for which they are not properly trained. In the author's own experience when he was in the Navy, he was often given the role of Information Assurance Officer for a system or office but never given the training for it. He was often told that there was no money for it or that he was expected to learn it from his own initiative. However, shortly before he retired in 2005, the DoD CIO issued a policy, DOD Instruction 8570.1. [16] This policy mandated and standardized IA training requirements and standards. It listed classes of IA workforce members (e.g. managers, system administrators, CND analysts, etc.) and stipulated what training and certifications were needed for the positions. It is essential that to properly implement the 20 Critical Security Controls, technical staff need to understand basic security concepts and have the required technical competency. Therefore, just as DoD established a policy stipulating

what training and certification is required, so should CFX as part of its IA Awareness Program for the technical staff.

- Establishing appropriate training for the position role/level: In order to ensure effective training and awareness, the developers of the IA Awareness Program need to analyze the training needs of the staff by their roles and levels with the organization. For example, if a senior staff member is responsible configuration management, that member needs to be trained in Critical Controls 1, 2 and 3 as a minimum since they are directly relevant for that role.

Taken together, by accounting for the above-listed factors, the program developers will help ensure IA Awareness Program success.

4.3 Implementing the IA Awareness Program

After the Steering Committee reaches a consensus on the development of the program and its implementation, the committee then needs to submit the program plan for senior management approval. Usually, projects like this one will be assigned a Senior Vice President (SVP - sometimes referred to as a Partner) to oversee the project and have approval authority. The leaders of the Steering Committee will perform a formal presentation for the SVP who will then grant authorization for Firm resources or make recommendations for improvement, which may result in another meeting. After authorization is granted, the leaders of the Steering Committee will then set the logistics in motion for implementing the program and commence training.

As part of the implementation, the Steering Committee should develop an execution plan, showing how the plan will be carried out within the Firm. Appendix A shows how such an execution would look like in this scenario.

N.B.: This case study is based on a template from the CD-ROM that came with the SANS ISM 5300 course. [15] Throughout the course of the case study, there will be discussion on how elements of the IA Awareness Program are related to specific Critical Security Controls.

5.0 Conclusion

In the course of the author's work as an Information Assurance consultant, he has too often seen problems caused by organizations that fail to implement basic security controls. In fact, most Red Teams do not even bother to use hacking tools that hard are to come by or require highly advanced skills to use. They usually use hacking tools that are easily obtainable from the Internet for their testing for security vulnerabilities. In the author's conversations with Red Team members from various agencies and military services during conferences such as the Red/Blue Team (REBL) Symposiums, they have consistently said that they rely more on social engineering skills and their experience on how IT personnel often make security-related mistakes than hacking tools. This is consistent with the fact the 20 Critical Security Controls originated from the inputs of the NSA Red Team.

After examining the 20 Critical Security Controls, it becomes plain to see that all organizations that use information technology would be wise to implement the controls. As part of implementing these controls, this paper will demonstrate how to develop and execute an IA Awareness Program for the Technical Staff for a large consulting firm so they can fulfill their roles successfully. It is very important that an IA Awareness Program become one of the controls in of itself. The author hopes that this approach will serve as a successful example for other large organizations.

References

[1] Kleiner, A. (2004). *CFX: Helping Clients Envision the Future.* Old Saybook, Connecticut: Greenwich Publishing Group, Inc.

[2] Bennett, D and Riley, M. (2013, June 20). CFX, the World's Most Profitable Spy Organization. *Bloomberg BusinessWeek*. Retrieved from http://www.businessweek.com//2013-06-20/the-worlds-most-profitable-spy-organization.

[3] Kirk, J. (2014, June 9). *Numerous Groups Use Elderwood Hacks.* Computerworld, Retrieved June 28, 2014 from http://www.computerworld-digital.com/computerworld/20140609?pg=6#pg6.

[4] Defense Industrial Base (DIB) Cyber Security / Information Assurance (CS\IA) Program, (N.D.). Retrieved from http://dibnet.dod.mil/.

[5] *Critical Security Controls: A Brief History.* (N.D.). http://www.sans.org/critical-security-controls/history.

[6] Dittmer, J. Personal conversations, (2009 – 2011). Personal note: The author had personally supported Mr. Kevin Bingham, the former DoD Computer Network Defense Architect, from 2009-2011, as a contractor.

[7] Centre for the Protection of National Infrastructure, (N.D.). http://www.cpni.gov.uk/about/context/.

[8] Barlett, J. (2005). *How the 80/20 Rule Helps Us be More Effective*. Retrieved from http://www.pinnicle.com/Articles/Pareto_Principle/pareto_principle.html.

[9] Chabrow, E. (2012, January 13). *State Department's Streufert Moves to DHS*. Gov Info Security, Retrieved May 7, 2014 from http://www.govinfosecurity.com/state-departments-streufert-moves-to-dhs-a-4405.

[10] *Top 20 Critical Security Controls*. (N.D.) SANS Institute. Retrieved May 7, 2014, from http://www.sans.org/critical-security-controls/controls/.

[11] Rashid, F. Y. (2013, June 25). Organizations Implementing, Seeing Benefits of Critical Security Controls: Survey | SecurityWeek.Com. Retrieved from http://www.securityweek.com/organizations-implementing-seeing-benefits-critical-security-controls- survey.

[12] Verizon. 2014 Data Breach Investigations Report. Retrieved June 14, 2014, from http://www.verizonenterprise.com/DBIR/2014/.

[13] Hietala, J. D. (2013). Implementing Critical Security Controls. Retrieved from http://www.sans.org/reading-room/analysts-program/implementing-critical-security-controls.

[14] Spitzner, L. (N.D.). SANS Securing the Human: Security Awareness for the 21st Century. Retrieved May 9, 2014, from https://www.securingthehuman.org/media/resources/pdfs/security-awareness-brochure.pdf.

[15] SANS MGT 433/ISM 6000 – Communications Plan Lab, 2013. Retrieved May 9, 2014, from https://www.securingthehuman.org/media/resources/pdfs/security-awareness-brochure.pdf.

[16] Department of Defense Directive 8570.01. Retrieved July 15, 2014, from http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf.

Appendix: Consulting Firm X's Information Assurance Awareness Program for Technical Staff – Sample Execution Plan

Last Updated: 22 July 2014

Disclaimer: This proposed execution plan is part of an academic exercise and it has not been officially approved nor endorsed by any real consulting firm. This plan is based on publically obtainable information and does not contain any proprietary information. The author is a former employee who is no longer affiliated with CFX.

Table of Contents

1. Executive Summary

Our Firm takes the security of our organization, clients, users and data extremely seriously. To help protect our sensitive assets we have an active security awareness and education program in place. The goal of this long-term program is to not only to meet all compliance and legal requirements, but also to secure technical staff (CFX employees and contractors alike) and the organization by changing their behaviors. This document explains the recommended rollout and execution of a security awareness and education program for all of employees, staff and contractors.

The key objectives of this program are providing CFX IT technical staff with the following:

- *Keeping technical staff informed of the most current security practices and procedures.*
- *Ensuring that technical staff members are proficient in their tasks, especially those technical staff members with security related duties.*
- *Preventing security incidents by informing staff of proper security procedures.*
- *Enabling technical staff to respond to security incidents.*

The scope of this awareness program is to provide cybersecurity training and education for internal CFX IT technical staff and the contractors supporting them.

2. Steering Committee

The senior leadership of CFX has formed a Security Awareness Steering Committee (SC) made up of various members from the organization. The role of the SC is to assist the Security Awareness officer, with planning, executing and maintaining a successful and engaging program. Current committee members are:

John Johnson	Larry Hudson	Jonathan Chou
Tony Robertson	Rick Allman	Kim Quintanta
Dennis Gilbertson	Karin Fitzpatrick	Cam Trainor

Notes:

The program falls under the oversight of Joseph Mackson, Executive Vice President and Chief Information Security Officer of CFX. He is the program sponsor and he has ultimate responsibility.

The Project Manager for the IA Awareness Program is John Johnson, an Associate who received his Cybersecurity Expert Belt in 2013.

3. Target Audience

The first step is to identify our constituents that must complete the training. Within that overall group we then need to identify different targets, these sub-groups require additional training due to their daily activities. The recommended target groups are:

- **CFX IT Staff:** This is the core group for our security awareness and education program. We recommend that anyone with an organizational email address be required to be part of the awareness and education program. In addition, these individuals have privileged access to, maintain any servers, applications or network related equipment. This group includes contractors.
- **CFX Information Assurance Staff:** This is a subset of the IT Staff. The primary core competencies of these personnel are to protect the Firm's information infrastructure and the sensitive information belonging to the Firm and our clients.
- **CFX Service Desk**: This category includes any individuals that provide support to our internal staff or customers.

Languages possibly required for training materials include English (both American & British versions), French, German, Arabic and Korean.

4. Content of IA Training

The following is the training content that we recommend for each target group. This training was selected by completing a gap analysis to see which skills employees need and which behaviors employees are not adhering to in according with Critical Security Control 9-1. This included those risks based on the top human attack vectors. We then prioritized the topics and selected those topics that reduce the greatest amount of risk to our organization. (Note: Passages about mapping to specific Critical Security Controls refer to those describes at the SANS web site at: http://www.sans.org/critical-security-controls/controls)

Basic IA Awareness (What every employee should know, regardless of position)

You Are The Target: Employees often believe they are not a target, exposing the organization to tremendous risk. They often make assumptions based on such factors as their position in the Firm, the type of data that they process or their obscurity. This module addresses that misconception by explaining how they are under attack and why. In addition, we explain that that this training will not only protect them at work, but at home as well. This engages people, helping ensure the success of the organization's security awareness program. (Covers Critical Security Control 9 – 3)

Social Engineering: Many of today's most common cyber-attacks are based on social engineering. As such, we explain what social engineering is, how attackers fool people and their indicators. We then demonstrate a common social engineering attack. We finish with how people can detect these attacks and how to respond to them. (Covers Critical Security Control 9 – 3)

Email & Messaging: One of the primary means of attacks and exploitation is through email. Email is used for both simple, large-scale attacks and more targeted spear phishing attacks. We explain how these attacks work, including recent examples of phishing, spear phishing, malicious attachments and links and frauds. We then explain how to detect and stop these attacks. (Covers Critical Security Control 9 – 4)

Browsing: The browser has become the gateway to the Internet; it is the primary tool that employees use for online activity. As such, browsers and their plugins have become a common target for attackers. We teach people how to browse safely, including keeping the browser and plugins updated, avoiding bad neighborhoods, being careful of and scanning what they download. (Covers Critical Security Control 9 – 3)

Social Networking: Social networking sites have exploded in popularity, with staff sharing all sorts of private information about themselves and work. Cyber attackers know this and use this information for identity theft, spreading malware, frauds and even targeted attacks.

We discuss these risks and the steps your employees can take to protect themselves and the organization. (Covers Critical Security Control 9 – 3)

Mobile Device Security: Today's mobile devices (like tablets and smartphones) are extremely powerful. In most cases, these devices have the same functionality, complexity and risks of a computer, but with the additional risk of being highly mobile and easy to lose. We cover how to use mobile devices safely and how to protect the data on them. We will also cover the installation and operation of security software, which is mandatory for all CFX employees in order to access Firm resources via personal mobile devices. (Covers Critical Security Controls 7 - 1 through 7 - 10)

Passwords: Passwords are the "keys to the kingdom" and employees must guard them well. We cover what passwords are, why they are important and what makes a strong password, with an emphasis on passphrases. In addition, we cover how to protect and safely use passwords, including the use of different passwords, password managers and not sharing passwords with others. In addition, we will cover how passwords are managed within CFX. This training including requirements such as password length, types of characters allowed, change frequency, etc. (Covers Critical Security Control 16 - 8)

Data Security: Organizations have a tremendous amount of sensitive information that they must take extra steps to protect. This module explains these steps, including the use of only authorized systems to store or process sensitive information, restrictions on transferring or sharing such information and requirements for securely storing, transmitting and disposing of sensitive data. (Covers Critical Security Controls 17-1, 17-2, 17-3, 17-4, 17-5, 17-6, 17-7)

Working Remotely: For many organizations, employees are no longer working at the office. Instead, they work from home or on the road while traveling. Since organizations no longer have physical control of the user's work environment, there are unique risks. This module focuses on how these employees can protect themselves, including laptop security and creating a secure, mobile working environment. (Covers Critical Security Controls 7 - 1 through 7 - 10)

Physical Security: While physical attacks against your data are less likely to happen, when they do occur they can have a greater impact on the organization. In this module, we explain how attackers will attempt to trick and fool their way into restricted areas through social engineering. We also discuss how employees can protect the physical security of your facilities. (Covers Critical Security Controls 20-3 and 20-5. Although the CSCs do not directly address physical security itself, they do discuss block access via social engineering.)

User Incident Response: No matter how effective a security team and their processes are, there will be incidents. This module focuses on how employees can identify and report

an incident. We cover things to look for, such as suspicious activity or virus alerts and to whom to report an incident. (Covers Critical Security Controls 5-10 and 18-1 through 18-7)

Optional - Protecting Your Personal Computer: Security is not just an issue at work, but at home. In this module, we cover steps people can take to protect their personal computers, including the importance of updating their operating system, applications and plugins, the use of anti-virus and firewalls and the importance of backup. By building good security behaviors at home, people are more likely to follow them in the organization. (Covers Critical Security Controls 5-1, 5-3 and 5-4)

Advanced training for IT Technical Staff (e.g. System Administrators, Service Desk personnel, etc.)

Password Resets and Administrative Account Password Management: Often users lose passwords or cannot login into their accounts or applications via their normal passwords. In addition, users leave security open by using accounts with administrative privileges unnecessarily. We will cover procedures to authenticate users and assist them in resetting their passwords. In addition, this training will cover topics like managing administrative and device account passwords. (Covers Critical Security Controls 12-1 through 12-9)

Smart Card Assistance: As CFX transitions all of its users to using their smart cards as their primary means of authentication, our Service Desk staff need to be trained to assist users to use their smart cards. (Covers Critical Security Controls 12-1, 12-13 and 16-14)

Managing User Accounts: Often cyber-attacks are done using old accounts or those for which passwords have not been updated in a long time. We will cover procedures for properly managing accounts including encryption, multi-factor authentication and audit logging. (Covers Critical Security Controls 16-1 through 16-17)

Managing Applications: In a large and geographically dispersed Firm like CFX, there are many applications and versions used by our employees. Often, non-standardized applications that are not supported lead to security vulnerabilities. In addition, there are outdated versions that may present security vulnerabilities. We will train personnel about our corporate whitelisting procedures with respect to how to support and secure approved applications. In addition, secure application software development and maintenance will be included in this training. (Covers Critical Security Controls 6-1, 6-3, 6-4, 6-10 and 6-11)

Conducting System Scans & Mitigation Activities: All too often, security vulnerabilities are created when technical personnel have not updated security controls, including patching system software. We will train system personnel on the scan-mitigate-scan procedures and processes so they will become part of the regular routine. As part of the mitigation process,

technical personnel will be trained how to properly test software and patches before going live. (Covers Critical Security Controls 4-1 through 4-10, 17-6 and 20-6)

Incident Handling & Response Activities: Despite all precautions, security-related incidents will happen and CFX, as a firm, needs to be able to respond to them in a professional manner while doing our best to support our users and clients. This training will cover topics such as incident handling and response, mitigation activities, continuity of operations and disaster recovery. (Covers Critical Security Controls 5-10 and 18-1 through 18-7)

Configuration Management for Hardware and software: Security vulnerabilities often arise from devices and software that are outdated, unauthorized, not currently patched, etc. In addition, as users utilize wireless networks and bring their own devices to the work environment, the potential for security incidents grows. As a result, IT staff must be diligent about controlling the configuration of network devices and software. The training will train IT staff on the processes and procedures to ensure that only authorized, properly patched and configured devices and software operate on the CFX networks and systems. Part of this training will cover using scanning and inventory tools as well as whitelisting procedures. (Covers Critical Security Controls 1-1 through 1-7, 2-1 through 2-9, 3-1 through 3-10 and 10-1 through 10-6)

Continuous Vulnerability Assessment and Remediation: Since monitoring and mitigating vulnerabilities is a full time security function, IA personnel need to be trained on the processes, procedures and tools to monitor and mitigate for security vulnerabilities. (Covers Critical Security Controls 4-1 through 4-10)

Management of Network Ports, Protocols and Services: Just as improperly configured hardware and software create security vulnerabilities, improperly managed networks ports, protocols and services leads to security issues as well. In this training, IA staff will learn how to use the processes, procedures and tools to monitor and mitigate for security vulnerabilities among the network ports, protocols and services. In addition, personnel will be trained how to monitor and control network accounts. (Covers Critical Security Controls 11-1 through 11-7, 16-1 through 16-17)

Computer Incident Response Team (CIRT) Training: Working in a CIRT requires specialized, in-depth skills such as Network Monitoring, Boundary Defense, Malware detection, Incident Response and Handling, etc. In addition, CFX CIRT personnel will be trained in Data Recovery and Business Continuity processes to ensure continuous operations during security incidents. In this course, CFX CIRT will learn those skills and how to employ them within the Firm. (Covers Critical Security Controls 5-10, 8-1 through 8-4, 13-1 through 13-14, 14-1 through 14-10 and 18-1 through 18-7)

Secure Network Engineering: Since CFX personnel develop systems for our clients or provide services for them, we need to rebuild or update our systems with secure network engineering process in mind. This type of engineering requires a great deal of knowledge about security processes and architectural principles. Therefore, it requires training for our security and system engineers/architects. (Covers Critical Security Controls 19-1 through 19-4)

Penetration Testing and Red Teams: In order to provide better security for our networks, our IA staff needs to conduct frequent scans and penetration tests. However, that is not enough. Our CIRT and our networks must have defenses tested by security experts from Red Teams who might consist or CFX or contractor personnel. This course will cover preparation and testing procedures. (Covers Critical Security Controls 20-1 through 20-8)

Understanding and Implementing the 20 Critical Security Controls: The course is meant to give IA personnel a basic understanding of the 20 Critical Security Controls, their purpose and how to implement them within CFX. (Indirectly covers all Critical Security Controls)

5. The Program's Approach

This program will be communicated in a positive manner. We will not focus on Fear, Uncertainty or Doubt (FUD). Instead, our focus will be on how the training not only protects our people and clients at work, but protects them at home, how this this will enabled them to use technology more effectively in their daily lives. Not only does this approach create an engaging program where people come to us, but also we have the potential of changing their behaviors not only at our organization but also at home.

5.1 New Hires

All new CFX employees and contractors are required to complete the online security awareness training course within 15 days following the issuance of their organizational email account. The CFX CIRT will enforce this policy. Any new hire or contractor who has completed their online awareness training within three months of the annual training do not have to take the annual training. (Covers Critical Security Control 9-3)

5.2 Training

Annual Training: The primary method we will use to communicate our program is annual online video training through our internal Learning Management System. During online training, all users will also take an online quiz to test comprehension of each module. This annual training will be required for all staff and contractors during the month of October each year. The CIRT will assume operational control of online awareness training and enforce this policy. This training will be in addition to any training required by clients as stated in contracts such as the DoD Cyber Challenge. (Covers Critical Security Control 9-3)

Reinforcement Training: Throughout the rest of the year, we will send quarterly newsletters, each newsletter reinforcing a specific topic from our primary training. Once we have established the program we will then deploy optional additional materials, including stickers, blogging, posters and corporate intranet webcasts. (Covers Critical Security Control 9-3)

5.3 Closing Accounts

When a CFX employee or contactor leaves the Firm, their access to the corporate on-line resources is removed. These steps will be added to the IT and Human Resources standard closing out processes. (Covers Critical Security Controls 16-1 through 16-4)

6. Feedback and Improvement

Our security awareness and education program is a long-term project. As such, we need a process to continuously update and improve our program.

Feedback Evaluations: We recommend that twice per year we send out feedback evaluations to receive input from end-users on how we can improve the program, once after annual online training and once six months later. Key points would include what they like the best about the training, what they feel is in need of improvement, what one thing they learned and what behavior the changed because of that.

Steering Committee Meetings: Plan SC meetings once a quarter to discuss the progress of the training and what we can do to improve. The SC will then review our training matrix and identify any new modules that need to be added, any old modules that need to be removed or any existing modules that need to be updated based on our compliance, legal and risk reduction requirements. Any modules identified as needing to be updated will have their learning objectives document reviewed and then modified accordingly. Once that is done, all content/media relevant to that module will be updated according to the new learning objectives.

7. Testing & Metrics

To ensure we are effectively educating users and changing their behaviors we need to test. We recommend the following methods to measure the impact of our training.

Surveys: The Firm Training Department will send out a bi-annual awareness survey to test user understanding of policies, standards and understanding of security issues. (Covers Critical Security Controls 9-1 and 9-2)

Phishing Assessments: the CFX CIRT will have monthly phishing assessments to test users' ability to identify and avoid falling victim to social engineering attacks. We recommend that we let employees and staff know that such phishing assessments will be happening.

- We communicate the fact that this training is for people's benefit. Management will not see the results of the assessments unless someone is a repeat offender.
- Phishing emails will replicate common attacks. If someone has fallen victim, that person will be immediately notified.
- 24 hours after every awareness assessment, we send out an email to all staff explaining the phishing email that was sent out, how many people fall victim and how they could have determined it was a phishing attack.

We recommend the following policy on failures.

- For the first failure in a year, the individual is notified and explained what they did wrong.
- For the second failure in a year, the individual is notified, explained what they did wrong and will receive additional training.
- For the third failure in a year, the individual is contacted, explained what they did wrong, receive additional training and disciplinary action. In addition, they are reported to management as a high-risk employee.

8. Key Dates and Milestones

Below are the timeline and key milestones for our initial web and classroom based training rollout. Once we accomplish this, we will shift focus to monthly updates and reinforcement training. Human Resources will be responsible for ensuring any new hires take the online training.

01 Sep 2014:

Identify all Technical Staff and create required mail lists.

Initial security awareness survey to establish a baseline

30 Sep 2014: – Initial email from CEO to all staff officially announcing security awareness program.

06 Oct 2014: – Training loads all accounts from the awareness mail list to the LMS. The LMS will then automatically send login accounts sent to all staff. All staff required to complete training by end of month.

31 Oct 2014: – Reminders sent to everyone who has not completed training.

01 Nov 2014: – Begin monthly newsletters and monthly phishing assessments.

07 Nov 2014: – Report sent to the CISO on who has and who has not completed training.

Last Updated: October 24th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, AE	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, NL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Miami 2017	Miami, FLUS	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
GridEx IV 2017	Online,	Nov 15, 2017 - Nov 16, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CAUS	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, GB	Nov 27, 2017 - Dec 02, 2017	Live Event
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZUS	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Khobar 2017	Khobar, SA	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TXUS	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, DE	Dec 04, 2017 - Dec 09, 2017	Live Event
European Security Awareness Summit & Training 2017	London, GB	Dec 04, 2017 - Dec 07, 2017	Live Event
SANS Bangalore 2017	Bangalore, IN	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Frankfurt 2017	Frankfurt, DE	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DCUS	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS SEC460: Enterprise Threat Beta	San Diego, CAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS San Diego 2017	OnlineCAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced