Global Information Assurance Certification Paper

United Airlines May 2015 Data Breach: Suggested Near, Mid and Long-Term Mitigating Actions Using the 20 Critical Security Controls

GIAC (GSLC) Gold Certification

Author: Philip G. Rynn, scholar59@hotmail.com
Advisor: Barbara L. Filkins
Accepted: November 10, 2015

Template Version September 2014

Abstract

In May 2015 it was widely reported that United Airlines detected a systems breach that compromised its customers' flight records, in addition to other data. This theft of passenger manifests is believed to have been perpetrated by the same attackers that stole up to 21.5 million social security numbers from the U.S. Office of Personnel Management (OPM) and medical records from Anthem Blue Cross in 2014-2015. Using open-source internet research methods, this paper examines the nature of the breach, and proposes specific near, mid and long-term actions that should be taken by United Airlines' senior security staff, using the Top 20 Critical Security Controls, to mitigate the impact of the system breach and to reduce the likelihood of further incidents. This paper is written from the view of an external security consultant addressing United Airlines' senior security staff via a formal, written report.

1. Introduction

A series of highly-publicized data breaches in recent years have shed light on the growing threat and prevalence of private and public organizational loss of valuable on-line data at the hands of illegitimate sources. According to the Center for Strategic and International Studies (CSIS), "…the likely annual cost to the global economy from cybercrime is $400 billion," with the economies of the United States, Germany, Japan and China accounting for half of that total (CSIS, 2014). The same study points out that the United States suffers one of the highest annualized loss rates as a percentage of Gross Domestic Product, third only to Germany and the Netherlands (CSIS, 2014). While there are regional variances in the degree to which cybercrime losses can be accurately determined, U.S. cybercrime loss estimates are considered fairly reliable due to the U.S. government having made a better effort to identify what theft of intellectual property has occurred due to foreign hackers (CSIS, 2014).

Cybercrime can take many forms. Hacking, theft of intellectual property, cyber-stalking, identity-theft, and introduction of malicious software are some of the most common (Cross Domain Solutions, n.d.). Hacking is undertaken for a number of reasons, including state-sponsored hacking, which is practiced by foreign governments for military advantage (Siciliano, 2011). As one Chief Information Security Officer commented in *Security Affairs*, "the line between cybercrime and cyber warfare is thin, we have [to understand] that one of the main strategies pursued by governments around the world is to make intelligence operations through technology [in order] to gather sensitive information relating to private industry and military sectors that somehow represent the backbone of the nation…cyber espionage is a terrible cyber threat [that] can have devastating effects on the social fabric of a nation as well as on the actions of every private company" (Paganini, 2012).

The recent breach at United Airlines (UA) is one in a long line of high-visibility data breaches that have had an impact on both private industry and public institutions – not only in the United States, but globally. This report will highlight the nature of the UA breach, and compare it to several well-known recent breaches that likely share a common

attack vector. The key findings that are common to all of the breaches will be discussed, and a list of recommended actions, using the *Critical Security Controls for Effective Cyber Security* (Council on Cybersecurity, 2014) will be proposed to UA senior management in an effort to implement near, mid and long-term controls that mitigate the immediate impact of the recent breach, and that implement relevant security controls as part of UA's cybersecurity strategy.

2. Situation

This situational analysis describes what is known about the United Airlines breach, how the breach is linked to other noteworthy breaches, and provides an in-depth evaluation of the probable common attack signature.

2.1. What Is Publicly Known About The UA Data Breach

In May or early June of 2015, officials at United Airlines detected an incursion into its computer systems (Riley & Robertson, 2015). Authorities determined that the incursion resulted in the theft of flight manifest data, which included information on passengers and their destinations (Security Experts, 2015). Potential motives for the attack remain under investigation by United Airlines authorities (Palmer, 2015), but several have been suggested by leading security practitioners familiar with the nature of the breach:

- Ken Westin (Senior Security Analyst at Tripwire): "Instead of a campaign to breach a single entity, the goal was to compromise multiple disparate sets of data for the purposes of correlation. This correlation would allow the actors to develop targeted profiles of the individuals in the United States, particularly those with security clearances, leading to one of the most devastating intelligence compromises we have seen to date" (Palmer, 2015).
- Jeff Hill (Marketing Manager at STEALTHbits): "Analyzing the travel habits of U.S. Government personnel can somewhat harmlessly provide insight into the development of new alliances or business partnerships, but can also be an invaluable tool in the never-ending effort by intelligence agencies to

compromise those with access to classified information. Despite the sophistication of high tech satellites, ground-based signals collection and monitoring devices, and other technology, the best intelligence is still obtained from the mid-level government employee desperate to keep his overseas fling a secret" (Security Experts, 2015).

- Kevin Foisy (Chief Software Architect and co-founder of STEALTHbits): "The bigger picture is the know-how being gained in the ongoing successful penetration of infrastructure. These are undoubtedly training grounds for the real attacks that could come in the event of war" (Security Experts, 2015)

Official details of the attack vector on UA systems are relatively non-existent. More has been published about recent breaches at Anthem and the United States Office of Personnel Management (OPM), and strongly suggests that the UA breach shares the same threat actors, threat vectors, and attack signatures as the aforementioned breaches (Constantin, Palmer, Rashid, 2015).

2.2 Linkage of UA Data Breach to Previous Data Breaches

Bloomberg reports that the hacker group is believed to have ties to the Chinese government and also broke into the computer systems of at least 10 other companies and organizations, including Anthem Blue Cross (Constantin, 2015). It was also reported that the breach may have been discovered with the help of investigators of the United States Office of Personnel Management (OPM) breach, who built a list of other potential victims after analyzing the domain names, phishing emails and attack infrastructure used by the hacker group (Constantin, 2015). United Airlines was included on that list (Riley & Robertson, 2015). According to one report, there was evidence that the hackers were in UA's network for months (Riley & Robertson, 2015). A web domain: UNITED-AIRLINES.NET was established in April 2014 and registered to a "James Rhodes" with an address in American Samoa (Riley & Robertson, 2015). The name "James Rhodes" is also the alias of a character in Marvel Comics' *Iron Man*, and security companies that tracked the OPM hackers stated that this hacker group often use Marvel comic book references as a way to sign their attack (Riley & Robertson, 2015).

While online news reports of the data breaches at United Airlines, Anthem and OPM suggest a common thread (Constantin, Kadlec, Palmer, Rashid, Secure Thoughts,

2015), there are no publicly-available reports detailing the exact way in which the data breaches occurred. OPM participated in a series of congressional hearings in June and July 2015 that were dedicated to its data breach, but limited the testimony on the actual mechanics of the breach event to closed-door, classified sessions with members of Congress (Congressional Testimony, 2015). However, recent published warnings by the Federal Bureau of Investigations (FBI) (Ragan, 2015) and reports by industry insiders and threat analysis groups that monitor the emergence of information threats point to the strong possibility that malware, in the form of a Remote Access Trojan named Sakula that originates from China, is the common threat vector behind these data breaches. (Threatconnect, Crowdstrike, Krebs, 2015).

2.3 The Sakula RAT

Remote Access Trojans (aka "RAT") are malware programs that include a back door for administrative control over a targeted computer. RATs are usually downloaded invisibly with a user-requested program or sent as an email attachment. Once that a host system is compromised, the hacker can use it to distribute RATs to other vulnerable computers (Rouse, 2009). The Federal Bureau of Investigation has warned that hackers responsible for malware intrusions employ a diverse selection of tools and techniques to attempt to gain initial access to a host system, including using credentials acquired during previous intrusions (HIPPA, 2015). Once that a RAT establishes administrative control of a computer, it allows for keylogging, access to PII (Personally Identifiable Information) such as credit cards or social security numbers, activation of the system's webcam and other recording interfaces, distribution of viruses and additional malware, formatting of drives, and the deletion, downloading, or altering of files and file systems (Rouse, 2009).

In late 2014, the threat analysis team at Crowdstrike reported on a campaign of targeted hacking events focused on the U.S. defense industrial base, healthcare, government, and technology sectors. The hackers infected victims with Sakula malware variants that were signed with stolen digital certificates (Crowdstrike, 2015). Additionally, the team's investigation into the activity led to associating it with activities performed by "Deep Panda" (Crowdstrike, 2015), which, according to the *Wall Street Journal*, is one of many names used by a state-sponsored Chinese cyber espionage group

(Krebs, 2015). Ongoing forensics into the Anthem breach also showed that the servers and tools used in the attack bore the common signature of the group (Krebs, 2015).

Crowdstrike also used their diagnostic tools and processes to determine that Deep Panda used an executable, which was not detected by anti-virus products (as late as 31 July 2014), which causes the victim (upon execution) to view a website by using the ShellExecute() API (Application Program Interface) to open a URL (Uniform Resource Locator). The site's domain name was meant to spoof that of a site set up to provide information on an alumni event for a U.S. University and requested that the visitor download an Adobe-related plugin in order to view the content (Crowdstrike, 2015). The downloaded plugin file included a variant of the Sakula malware (Crowdstrike, 2015).

Crowdstrike determined through further analysis that the same type of activity was conducted as far back as April 2014, when the same TTPs (Tactics, Techniques, Procedures) were used to target a healthcare organization and a U.S.-based information technology company with high-profile clients in the defense sector (Crowdstrike, 2015). Ostensibly, the healthcare organization targeted was Anthem (Krebs, 2015).

Further analysis by Crowdstrike revealed that all incidents in this Sakula malware campaign were similar in that they used malicious droppers masquerading as installers for legitimate software applications like Adobe Reader, Juniper VPN, and Microsoft ActiveX Control (Crowdstrike, 2015). The executables displayed progress bars that made it appear as if the specified software was being updated or installed (Crowdstrike, 2015). In addition, the droppers all directed victims to login pages for services specific to the target organization like webmail, document sharing, or a corporate VPN (Crowdstrike, 2015). In all cases except one, the victims were directed to login pages, the lone exception being when the victims were sent to a login page hosted on a domain that spoofed that of the legitimate one (Crowdstrike, 2015). It is unclear whether redirecting victims to these login pages was part of a credential-collection activity or merely meant to deceive victims into believing that the activity was legitimate (Crowdstrike, 2015).

3.0 Related Data Breaches

Philip G. Rynn, scholar59@hotmail.com

As mentioned previously, several breaches have been linked to the United Airlines breach due to the common attack vector and the attack source. Anthem and the United States Office of Personnel Management have also both suffered catastrophic breaches in the last 18 months. What follows is a description of their data breaches and a review of their efforts at remediation.

3.1 Anthem Data Breach

Anthem is the largest managed healthcare company in the Blue Cross Blue Shield Association, and one of the largest health care organizations in the U.S., providing healthcare coverage for about half of the federal workforce (Threatconnect, 2015).

3.1.1 Chronology of Events

On 4 February 2015, major news outlets broke the story that Anthem's network defenses had been breached (Threatconnect, 2015). According to a statement from Anthem's CEO the hackers "obtained" the PII of approximately 80 million customers (Threatconnect, 2015). The stolen information included social security numbers, dates of birth, residential addresses, phone numbers and income data (Threatconnect, 2015).

On 5 June 2015, the FBI released a memo detailing the type of malware used by threat actors that have compromised and stolen sensitive business information and PII, and while Anthem was not directly named in the alert, the FBI memo mentioned Sakula directly, and included 312 hashes of the malware (Ragan, 2015).

For the Anthem breach, the Sakula RAT used a stolen digital signature from the Korean company DTOPTOOLZ Co., and was configured to communicate with two fake command and control domains, extcitrix.wellpoint[.]com and www.we11point[.].com (Threatconnect, 2015). The domains were operationalized in April 2014 (Ragan, 2015). Threatconnect concluded that the malicious infrastructure was likely named in a way to impersonate the legitimate Wellpoint IT infrastructure, and additional Threatconnect analysis revealed that fake sub-domains such as hrsolutions.we11point[.]com were used to mirror legitimate remote infrastructure and employee benefits (Threatconnect, 2015). Threatconnect also concluded that "the malicious infrastructure closely mirrored other legitimate Wellpoint infrastructure [which] supported our hypothesis that the … Sakula malware was configured to operate and persist within a specific target enterprise" (Threatconnect, 2015).

3.1.2 Remediation Efforts to Date

In 2015, Anthem reportedly spent $65 million upgrading security, and planned to spend an additional $65 million while focusing on improvements in employee training, enhanced authentication procedures, implementation of passwords that expire every day, and retention of 55 experts who work on systems and defense upgrades (Seesel, Fields, Jorden, 2015). Additionally, Anthem's customers accepted an offer of free cyber insurance protection (Seesel, Fields & Jorden, 2015).

Anthem was covered under a tower of cyber insurance protection at the time of the breach, reportedly received the first-tier carrier claim, and seeked to collect from several more tier levels (Seesel, Fields & Jorden, 2015). In the wake of the breach, however, reports are that renewal of Anthem's cyber insurance coverage appeared to be cost-prohibitive (Seesel, Fields & Jorden, 2015). Thus, Anthem reportedly self-insured for the first $100 million of risk and obtained supplemental coverage from third-party carriers (Seesel, Fields & Jorden, 2015).

3.2 OPM Data Breach

The Office of Personnel Management performs personnel management functions for the U.S. federal government In addition to managing the federal personnel hiring system and policies, OPM conducts background investigations on federal personnel at the Secret and Top-Secret levels, maintains the security backgrounds for personnel that are granted clearances, manages the federal civil service merit system and pension benefits, including the pensions of retired federal employees, and provides federal employee training programs and management tools for the federal workforce (OPM, 2015).

3.2.1 Chronology of Events

On 5 June, 2015, the *Wall Street Journal* reported that the FBI was investigating the theft of up to four million personnel records from OPM (Barrett, Palleta & Yadron, 2015). In a 9 July news release, OPM stated that the types of information in these records included "Social Security numbers; residency and educational history; employment history; information about immediate family and other personal and business acquaintances; health, criminal and financial history; and other details" (OPM, 2015). Additionally, OPM reported that the breach discovery was extended to include a secondary breach that now affected 21.5 million individuals, and that the breach also

included the theft of 1.1 million fingerprints (Pagliery, 2015) (that number would later be revised to 5.6 million (Sanger, 2015)) (OPM, 2015).

Initially, *Fortune* magazine reported that the breach was detected during a product demonstration conducted by CyTech Services for OPM, using a vulnerability assessment tool called CyFIR (Hackett, 2015); CyTech Services published a report and stated that "CyFIR quickly identified a set of unknown processes running on a limited set of endpoints. This information was immediately provided to the OPM security staff and was ultimately revealed to be malware. CyTech is unaware if OPM security staff had previously identified these processes" (Irvine, 2015). OPM rebutted this claim, with a spokesman telling *Fortune* that OPM's cybersecurity team had made this discovery in April 2015 and had immediately notified US-CERT and the FBI to investigate the intrusion (Hackett, 2015). Dr. Andy Ozment, Assistant Secretary for Cybersecurity and Communications at the U.S. Department of Homeland Security, reinforced OPM's statement in congressional testimony that "as soon as OPM identified malicious activity on their network, they shared this information with the DHS…[we] then used one of our programs…to look back in time for other compromises across the federal civilian government. Through this process…[DHS] identified a potential compromise at another location with OPM data" (Ozment, 2015).

Throughout the month of June 2015, OPM Director Katherine Archuleta defended her agency's actions prior to and upon discovery of the breach (Archuleta, 2015), and directed OPM to take specific measures to immediately address near-term vulnerabilities, both through news releases and the release of a "Cybersecurity Action Report" (Office of Personnel Management, 2015). Measures included offering 18 months of free credit monitoring and identity theft insurance to personnel identified as having lost their data, (which was considered in line with typical private sector offers) (Peterson, 2015). As part of OPM's "defense" to Congress, Donna Seymour (OPM CIO) argued that legacy systems created an obstacle to security, and that in spite of OPM having encryption tools on hand, some systems could not be secured (Gallagher, 2015). Seymour stated: "some of [the systems] were written in COBOL, and they could not be easily upgraded or replaced. These systems would be difficult to update to include encryption or multi-factor authentication because of their aging code base, and they would require a full re-write"

(Gallagher, 2015). In 24 June testimony to Congress, Patrick McFarland, Inspector General (IG) of OPM, testified that "we know from our audit work that some of the OPM systems involved in the data breach run on modern operating and database management systems. Consequently, modern security technology such as encryption or data loss prevention *could* [emphasis added] have been implemented on these specific systems."

At the conclusion of the first Congressional hearing into the OPM breach on 16 June, House Oversight Committee Chairman Jason Chaffetz (R-Utah) told Archuleta and Seymour, 'You failed utterly and totally'" (Gallagher, 2015). Facing continued political pressure and calls from Congressional representatives to step down, Archuleta tendered her resignation on 10 July (Davis, 2015).

While the actual breach signature was never publicly disclosed during the June testimony (with Archuleta, Ozment and Seymour all steering the Congressional Committee members to a classified briefing on the breach protocol at the conclusion of the hearings (Miller, 2015)), follow-on testimony by Sylvia Burns, CIO of the Department of the Interior (DOI), during hearings (15 July) on DOI's role in the OPM breach, explained the fundamental way that the breach occurred. Said Burns: "the breach did not happen because of a vulnerability at the DOI data center. It happened *because of compromised credentials of a privileged user on the OPM side who then moved into DOI's environment through a trusted connection* [emphasis added]" (Mazmanian, 2015).

3.2.2 Remediation Efforts to Date

OPMs breach remediation efforts have focused on specific activities of four distinct efforts: OPM's planned assistance for individuals that were affected by the data breach (OPM, 2015), specific actions set forth in OPM's Cybersecurity Action Report (OPM, 2015), DHS' planned effort to incorporate OPM into its Continuous Diagnostics and Mitigation (CDM) program (Ozment, 2015) (DHS, 2015), and the Federal CIO's ongoing efforts to coordinate OPM's "Cyber Sprint" (Lyngass, 2015).

OPM determined that it would take the following measures to establish protection measures for individuals that were affected by the breach (OPM, 2015):

- Provide a comprehensive suite of monitoring and protection services for background investigation applicants and non-applicants whose social security numbers or in many cases other sensitive information were stolen.

- Help other individuals who had other information included on background investigation forms (through publication of best practices for protection, and publicly available resources).
- Establish an online cybersecurity incident resource center.
- Establish a call center to respond to questions.
- Protect all Federal employees (through development of a proposal for credit. and identify theft monitoring services that should be provided to all Federal employees in the future.

OPM's Cybersecurity Action Report laid out specific steps that would be undertaken in the near-term to "Bolster Security and Modernize IT Systems" (OPM, 2015):

- Improve security through completing deployment of two-factor authentication, expanding continuous monitoring (through the DHS CDM program), ensuring access to contractor systems (in the event of incidents), and reviewing encryption of databases.
- Leverage outside expertise through the hiring of a new cybersecurity advisor, consulting with outside technology and cybersecurity experts, and increasing consultations with the Inspector General.
- Modernize systems by migrating to a new IT environment, finalizing the scope of the ongoing migration process, further evaluating all contracting options, and requesting additional funding support from Congress.
- Strive for increased accountability, establishing regular employee and contractor training, documenting incident response procedures, and ensuring compliance with the Federal Information Security Management Act (FISMA).

OPM has also started work under a task order with DHS to implement the Continuous Diagnostics and Mitigation (CDM) program (Boyd, 2015), which institutes continuous monitoring over 15 diagnostic capabilities/areas, arranged by phases. Phase 1 will focus on hardware, software, configuration setting, and vulnerability management. Phase 2 will focus on access control, security-related behavior, credentials and authentication, privileges, and boundary protection management. Phase 3 will focus on

event planning, event response, audits/monitoring, documentation/policy, quality management, and risk management (DHS, 2015).

Tony Scott, Federal CIO coordinated a 30-day "cyber sprint" at OPM, which assessed the security of federal civilian and military IT networks post-breach, and is planning on publishing a "Cybersecurity Sprint Strategy and Implementation Plan (CSSIP)" by September/October 2015. Included in this plan is the adoption of common diagnostic and mitigation tools by all elements of the government (Lyngass, 2015).

4.0 Lessons Learned from United Airlines, Anthem and OPM Data Breaches

Due to the public nature of the OPM breach, its findings and remediation actions have been well-publicized. Congressional Testimony on the part of OPM and OPM's support structure (contractors and DHS) laid bare all of the systemic and procedural weaknesses that allowed the breach to occur, and that exposed OPM to catastrophic data loss. At the same time, OPM was very public in addressing the steps that it would take to remedy the incident, developing a comprehensive near-term plan to address immediate issues, while refocusing its efforts on completing long-term fix actions that were already underway.

Anthem's breach, while under less public scrutiny than the OPM breach, is still correlated to the Sakula RAT (as analyzed by Crowdstrike), and based on Anthem's public statements, seems to confirm the attack signature linkage to OPM's breach.

The United Airlines breach, which at face-value was not on the scale of the Anthem and OPM breach, provided a missing-link for the data thieves, in that the type of information stolen was complementary to the data thefts at Anthem and OPM, and which has now led to the prevailing thought that the Sakula RAT attack, at least when employed against Anthem, OPM and UA, was not for economic gain, but for espionage.

The following discussion highlights the key findings common to all three breaches, as a way to identify commonalities between all three entities that can be immediately remedied through selective implementation of the 20 Critical Security Controls.

4.1 Finding #1 - The last line of defense: "the user", failed

The Sakulat RAT malware, regardless of its deliberate attack protocol, still requires a network-authorized user to take a specific action on a device internal to a network. The user must simply click on an email attachment, or access a rogue site to allow the RAT to enable the hacker to gain a foothold into the network. Once in the network, the hacker can then use that machine as his pivot point to exploit other internal system or network vulnerabilities. In the well-documented case of OPM's breach, data encryption would still not have prevented the intrusion. As Dr. Ozment pointed out in his Congressional Testimony, the attackers had gained valid user credentials to the systems that they attacked, and due to the lack of multi-factor authentication on these systems, the attackers would have been able to use those credentials at will to access systems from within and potentially even from outside the network (Gallagher, 2015). Due to the nature of the Sakula malware, social engineering also likely led to its placement on Anthem and UA networks. When all is said and done, the organizations' overall security posture was not enough to negate the mouse clicks that introduced the Sakula RAT.

4.2 Finding #2 – Weak Authentication and Access Management

Neither OPM Congressional Testimony or Anthem/UA online findings explicitly detail the standard authentication measures employed within their internal networks, or the way in which access management, credentialing, or policy management occur. However, the fact that the Sakula malware could exist on Anthem and OPM networks for 8-14 months strongly suggests that existing authentication and password regeneration practices allowed for long-term malicious access. Additionally, the OPM Congressional Testimony, at a minimum, raises the question about the levels of access granted to privileged users – the full complement of an individual's most vital PII used for Secret and Top Secret investigations was likely accessible to users that did not require anything more than an authorized user name and password for access. With an internal breach followed by routine keylogging, hackers had access to this data for months. For United Airlines, this finding is not as strongly defined – front-line employees could routinely be required to access flight manifests during daily operations. Yet, indications are that the breached system included not only user names and flight details, but dates of birth (SecureThoughts, 2015). This calls into question how decisions were being made about data segregation practices, which is further addressed in the next section.

4.3 Finding #3 - Weak Data Classification and Segregation

In terms of "richness of data", the OPM breach was by far the most damaging of the three examined breaches; not only did the hackers make off with the personal details of 21.5 million individuals that either worked for or were seeking employment with the U.S. Federal Government, but it also included PII on millions of friends, relatives and overseas contacts (Rashid, 2015). The Anthem breach, which affects about 80 million people, and which is narrower in the scope of the PII seized, nonetheless included a sizable amount of PII for a large segment of the U.S. population. The United Airlines breach, on the other hand, appears restricted to names, dates of birth, and their presence on flight manifests – the value of this data being how it can be correlated with OPM and Anthem data for espionage purposes affecting U.S. national security.

Noteworthy to the OPM breach, and perhaps of like concern with the Anthem breach, is the fact that either 1) sensitive, private data was within reach of hackers pivoting within an organizational enclave, or 2) privileged user computers were granted external access permissions in a way that allowed the malware to establish a pivot – regardless of the IDS or IPS architectural layout or organizational access control policies. And, there was no evidence that organizational-wide risk assessments had factored-in these vulnerabilities into a documented risk-acceptance posture. The Congressional Testimony of OPM indicates that organizationally, they were aware that their security posture was in dire need of upgrading (Archuleta, 2015); in the case of Anthem, their recognition of inherent enterprise-wide vulnerabilities is less apparent. For United Airlines, this is (as of yet) still an unknown. Fundamentally, what they all shared was a security posture that did not hold up to the Sakula RAT, and that took too long to discover its presence before damage occurred.

4.4 Finding #4 –Defense in Depth not judiciously employed

The first three findings fundamentally point to gaps in the security postures of the organizations that were breached. While no organizational risk posture is 100% secure, the OPM breach (through its public scrutiny) exposed systemic weaknesses that were present at the very top of the organizational leadership, and which were also present at the "working level" of information security. Congressional testimony indicates that OPM was actually aware of their shortfalls, and were taking steps to remedy weaknesses in a

prioritized fashion (Archuleta, 2015). However, their efforts were literally "too little, too late". By the time that OPM was getting in line with the recommendations made by the OPM Inspector General, the Sakula breach had already occurred. As a private entity, Anthem did not, and United Airlines does not face the public scrutiny that OPM went through in assigning blame. However, it's reasonable to conclude that both Anthem and United Airlines were experiencing some of the same organizational dynamics that led to their unplanned risk exposure, and that contributed to the loss of their data.

5.0 Recommendations

When looking at the myriad of security issues that can affect an organization's security posture, the Council on CyberSecurity's Critical Security Controls presents an effective means of categorizing and identifying the critical factors necessary to resolve security issues across the broad spectrum of organizations. Understandably, remediation actions using the Critical Controls run the risk of being overwhelming in scope; with fix-actions being categorized in up to 20 sub-categories of controls, "solutions" could quickly overwhelm an organization's response capability. Clearly, security incidents need to focus on a prioritized set of controls for the most effective incidence response.

In order to focus on the fundamental security issues that can be assigned a limited set of controls for effective remediation, it is best to focus on the fundamental "event" that occurred at Anthem, OPM and UA: *malware was employed in a targeted attack against a user using social engineering, which resulted in a loss of valued data.* Based on the evidence of how the breaches occurred, there were deficiencies (at all three organizations) in their ability to protect against malware, in user actions to defend against malware, and in the way that data was stored (leading to loss of PII).

The nature of this breach calls for implementation of critical security controls in three priority areas: Malware Defenses (Critical Security Control (CSC) 5), Security Skills Assessment and Appropriate Training to Fill Gaps (CSC 9), and Data Protection (CSC 17). Undeniably, a wholesale review of all of the issues that go into a resultant data breach would also uncover other security controls that need to be addressed/strengthened, but the three aforementioned controls, and their proper

implementation, have the most potential impact for UA, both in terms of securing systems and data, and in exercising due diligence for the protection of PII.

The following discussion will focus on those three critical security controls, and will present an approach for their implementation at United Airlines. Implementation of the controls will be presented as near-term, mid-term, and long-term actions. For purposes of this review, near-term actions are considered immediate actions (0-6 months) that serve to both mitigate the effects of the known data breach, and that implement the most immediate critical protection measures. Mid-term actions are other significant actions that should be undertaken in the present budgeting cycle (i.e. within the next 12 months) to strengthen UA's security posture, and long-term actions are activities that should be addressed by UA as part of its ongoing security strategy implementation process (in the next 12-36 months).

5.1 Near-Term

Under the general assumption that United Airlines network and systems security staff are not presently employing the following Malware Defense, Skills Assessment/Training and Data Protection controls, the following Critical Security Controls (CSC) should be implemented immediately, using the following guidance from the *Critical Security Controls for Effective Cyber Defense* (Council on CyberSecurity, 2014) (Appendix A):

To better defend against malware, the organization should configure laptops, workstation and servers NOT to auto-run removable media content (CSC 5-3). Systems should also be configured to automatically conduct anti-malware scans upon the insertion of removable media (CSC 5-4). Additionally, UA should scan and block all e-mail attachments entering the e-mail gateway containing malicious code or files types that are deemed unnecessary for business operations. Scanning should occur before e-mails are placed in the user's inbox; this action extends to e-mail and web-content filtering (CSC 5-5).

To immediately address potential issues in the area of workforce security skills, the organization should perform a gap analysis on UA employee skill sets in responding to malware attacks originating from multiple vectors, and use this analysis to build a baseline training and awareness roadmap (CSC 9-1). Training should be used to

remediate any identified deficiencies in employee malware defense, and should either be led by UA senior staff, or by having external trainers provide the training "on-site" to reinforce its relevance to daily work functions (CSC 9-2). UA security staff should also routinely conduct "inoculation" tests of the workforce to measure their resistance to malware/suspicious e-mails. Follow-on training/testing should be targeted to employees that require remedial training (CSC 9-4).

To immediately enhance data protection, UA must conduct a data assessment to identify sensitive information requiring additional encryption and integrity controls (CSC 17-3). Additionally, UA should review any existing cloud provider data protection practices to identify potential vulnerabilities (CSC 17-4). To detect the unauthorized use of encryption (in order to bypass network security devices), UA should also monitor all outgoing traffic. (CSC 17-12)

5.2 Mid-Term

Within the present budgeting cycle (or at the most within the next 12 months), UA technical staff should employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers (CSC 5-1). Anti-malware software could exist on a cloud-based centralized infrastructure, or administrators can manually push updates to all machines in the UA enterprise. Updated systems should be verified and confirmed for signature updates (CSC 5-2).

UA should also develop/improve its security awareness program to include online training that focuses on individual actions to block commonly employed methods of intrusion. This training should be modular and convenient to train with. Also, the training needs to be routinely updated with the latest attack signatures, and should be required as mandatory yearly training for all employees. A monitoring system should also be in place to confirm training compliance (CSC 9-3).

Institution of a mid-term data protection advanced measure should focus on deployment of an automated tool on the network perimeter to monitor PII, keyword and/or other document exfiltration attempts across network boundaries, and should block

such alerts while alerting security staff (CSC 17-5). Periodic scans of server machines should also detect the presence of sensitive information leaks via clear-text (CSC 17-6).

5.3 Long-Term

United Airlines should undertake, as part of an ongoing cyber security strategy (typically within a 36 month execution period), advanced security practices that are budgeted for, trained to, and implemented. Advanced security practices imply an allocation of resources dedicated to advanced diagnostics tools, and more importantly, in increase in training commitment for system security practitioners to install, operate and maintain these advanced tools for a stronger security posture.

The *Critical Security Controls for Effective Cyber Defense* list Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), and Enhanced Mitigation Experience Toolkit (EMET) as anti-exploitation features that can provide a more comprehensive set of security features for United Airlines' applications and executables. UA should review these capabilities to determine the extent to which they can be implemented within UA's desired risk management framework (CSC 5-6). UA should also ensure that longer-term implementation of automated monitoring tools includes the use of behavior-based anomaly detection tools to complement traditional signature-based detection tools (CSC 5-8). Additionally, UA should acquire network-based anti-malware tools to identify rogue executables in network traffic, and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at a user endpoint (CSC 5-9). As part of standard incidence response processes, UA should supply security teams with samples of malware running on corporate systems that do not appear to be recognized by existing anti-malware software. Samples can then be provided to UA's security vendor for "out-of-band" signature creation and later be deployed to the enterprise by UA's system administrators (CSC 5-10). An additional measure by UA system security personnel can be to enable domain name system (DNS) query logging to detect hostname lookup for known malicious C2 domains (CSC 5-11).

To strengthen the capabilities of the I.T. security workforce, UA should use security skill assessments for designated mission-critical security roles, using real world

problems to measure competency and ultimately, mastery. This can extend to participation in on-line cybersecurity competitions to strengthen skill-sets (CSC 9-5).

As a means to harden the UA enterprise to future attacks and breach attempts, UA should plan and budget for hard drive encryption software for authorized mobile devices and for any system that holds sensitive data (CSC 17-1). Cryptographic devices and software should be configured to use publicly-vetted algorithms (17-2). Data movement between networks should only be accomplished using secure, authenticated and encrypted means (CSC 17-7).

To the maximum extent possible (based on business needs), systems should be configured so that USB tokens and/or USB hard drives are disabled. If business needs require some degree of USB connectivity, enterprise software should be employed that configures systems to allow only certain USB devices (that are uniquely identifiable and a controlled item), and that use automatic encryption of all data placed on that device. Inventory control must be maintained for all USB devices (CSC 17-8).

Long-term implementation of system security upgrades should also budget for the following:

- Use of network-based DLP [Data Loss Prevention] solutions to monitor and control the flow of data, and for anomaly detection (CSC 17-9).
- Allow only approved Certificate Authorities (CAs) to issue certificates within the UA enterprise (CSC 17-10).
- Perform an annual review of algorithms and key lengths in use for protection of sensitive data (CSC 17-11).
- Define roles and responsibilities related to management of encryption keys within the enterprise (CSC 17-14).
- Implement Hardware Security Modules (HSMs) for protection of private keys or Key Encryption Keys, wherever required (CSC 17-15).

5.4 Metrics and Testing

Concurrent with review and implementation of the recommended control measures set forth in sections 5.1 through 5.3, United Airlines security staff must implement a set of automation and effectiveness metrics that baseline their present

security posture in the three critical security control areas, and that implements ongoing effectiveness testing for both Malware Defense and Data Protection. Appendices B through D outline the measurable performance criteria set forth in *The Critical Security Controls for Effective Cyber Defense* that should be automated, measured for effectiveness, and tested for effectiveness, in order for UA to improve on baseline effectiveness results and reduce overall risk (Council on CyberSecurity, 2014).

In deciding how to implement automation and effectiveness metrics, United Airlines should review the performance criteria of the suggested metrics in the appendices, and determine what can be presently measured under existing operational conditions and if the means exist to presently measure them; it is not expected that all criteria can be measured immediately, but UA senior staff should institute an implementation strategy over the next 12-36 months that puts them in a position to be able to conduct full effectiveness testing and bring the security areas of Malware Defense and Data Protection under control. Additionally, Security Skills Assessment and Appropriate Training (CSC 9) metric development need to be prefaced by a comprehensive security skill-set inventory, determination of existing training shortfalls, planning for incorporation of both remedial and routine training using on-line training labs (and other training modes as necessary), budgeting for such training, and the implementation of these processes over time. A realistic measure of full implementation for a robust cybersecurity training package at a large organization like UA, tailored for both system/security administrators and operational/administrative staff, is around 24 months, but with proper allocation of existing human and technical resources, and with prioritization of effort towards the most vulnerable elements of the organization, training could begin within 3-6 months. If UA presently has an ongoing security program, the timeline may also be accelerated by re-focusing training efforts on the Critical Security Controls and re-orienting the corporate approach towards new metrics development and effectiveness testing.

5.5 Other Critical Security Controls for Consideration

Discussion of prioritized controls to address and remedy the immediate security risk considerations of United Airlines necessarily called for a strict limitation on identifying the most essential controls to mitigate both the effects of the data breach, and

to initiate processes for longer-term sustainment of a reduced risk posture. However, there are several other controls that merit review by UA security staff, and that will serve to augment the prioritized efforts by UA to improve enterprise security.

As stated in Finding #2 (Section 4.2), the malware that was likely involved in the Anthem and OPM breaches was resident in their systems for 8-14 months. Until US-CERT was able to identify this threat, and understand the threat signature (see page 9), there was no formal knowledge of the presence of this threat. Based on the timing of the first known campaign of the Sakula RAT, it is conceivable that the malware was inside of the UA perimeter for many months. Poor controls related to malware defense and security skills/training set the conditions for the breach to occur, but deficiencies in Controlled Use of Administrative Privileges (CSC 12) and Controlled Access Based on the Need to Know (CSC 15) would have exacerbated the impact of the breach, and allowed for long-term data siphoning/theft (Council on CyberSecurity, 2014).

United Airlines should review their policies and security practices as they relate to access control and administrative privileges, and institute relevant sub-controls as necessary.

6.0 Conclusion

This report examined the nature of the breaches at Anthem and the United States Office of Personnel Management in order to better understand the attack vector likely undertaken against UA during its May 2015 breach. Using *The Critical Security Controls for Effective Cyber Defense*, near, mid and long-term remediation actions using select controls were proposed, in order to address systemic security issues that were exposed by the breaches. Automation and effectiveness metrics, along with effectiveness testing procedures were proposed as a way for United Airlines to bring critical processes under control and to strengthen its overall security posture.

With proper implementation of the recommended controls, and by taking the additional recommended steps of metrics development/assessment and effectiveness testing, United Airlines can exercise due diligence in mitigating the impact of the security breach, and set a foundation for overall improvement in its security posture and overall security strategy.

Philip G. Rynn, scholar59@hotmail.com

References

Archuleta, Katherine (2015, June 16). *OPM: Data Breach, Hearings before the Committee on Oversight and Government Reform, United States House of Representatives*, 114th Cong., Statement of The Honorable Katherine Archuleta, Director U.S. Office of Personnel Management on June 16, 2015. Retrieved from https://oversight.house.gov/hearing/opm-data-breach/

Archuleta, Katherine (2015, June 24). *OPM: Data Breach II, Hearings before the Committee on Oversight and Government Reform, United States House of Representatives*, 114th Cong., State of The Honorable Katherine Archuleta, Director U.S. Office of Personnel Management on June 24, 2015. Retrieved from https://oversight.house.gov/hearing/opm-data-breach-part-i/

Barrett, Devlin, Palletta, Damian &Yadron, Danny (2015, June 5). *U.S. Suspects Hackers in China Breached About 4 Million People's Records, Officials Say.* retrieved from http://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888

Boyd, Aaron (2015, June 19). *OPM breach a failure on encryption, detection*. Retrieved from http://www.federaltimes.com/story/government/omr/opm-cyber-report/2015/06/19/opm-breach-encryption/28985237/

Burns, Sylvia (2015, June 16). *OPM: Data Breach, Hearings before the Committee on Oversight and Government Reform, United States House of Representatives*, 114th Cong., Testimony of Sylvia Burns, U.S. Department of the Interior on June 16, 2015. Retrieved from https://oversight.house.gov/hearing/opm-data-breach/

Burns, Sylvia (2015, July 15). *Cybersecurity: The Department of the Interior, Hearings*

before the Committee on Oversight and Government Reform, Subcommittee on Information Technology and Subcommittee on Interior, United States House of Representatives, 114th Cong., Testimony of Sylvia Burns, Chief Information Officer, U.S. Department of the Interior, on July 15, 2015. Retrieved from https://oversight.house.gov/hearing/cybersecurity-the-department-of-the-interior/

Constantin, Lucian (2015, July 30). *OPM, Anthem hackers reportedly also breach United Airlines.* Retrieved from http://www.pcworld.com/article/2954872/opm-anthem-hackers-reportedly-also-breached-united-airlines.html

Center for Strategic and International Studies (CSIS) (2014, June). Net Losses: Estimating the Global Cost of Cybercrime. Retrieved from http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

Council on Cybersecurity (2014). *The Critical Security Controls for Effective Cyber Defense. (Version 5.0)*. Retrieved from https://www.sans.org/media/critical-security-controls/CSC-5.pdf

Cross Domain Solutions (n.d.). *Cyber Crime*. Retrieved from http://www.crossdomainsolutions.com/cyber-crime/

Davis, Julie H. (2015, July 11). Katherine Archuleta, Director of Office of Personnel Management, Resigns. Retrieved from http://www.nytimes.com/2015/07/11/us/katherine-archuleta-director-of-office-of-personnel-management-resigns.html?_r=0

Department of Homeland Security (DHS) (2015, September 14). *Continuous Diagnostics and Mitigation (CDM)*. Retrieved from http://www.dhs.gov/cdm

Philip G. Rynn, scholar59@hotmail.com

Esser, Michael R. (2015, June 16). *OPM: Data Breach, Hearings before the Committee on Oversight and Government Reform, United States House of Representatives*, 114th Cong., Testimony of Michael R. Esser, Assistant Inspect General for Audits, on June 16, 2015. Retrieved from https://oversight.house.gov/hearing/opm-data-breach/

Gallagher, Sean. (2015, June). *Encryption "would not have helped" at OPM says DHS official*. Retrieved from http://arstechnica.com/security/2015/06/encryption-would-not-have-helped-at-opm-says-dhs-official/

Hackett, Robert (2015, June 12). *A product demo may have revealed what could be the biggest ever government data breach*. Retrieved from http://fortune.com/2015/06/12/cytech-product-demo-opm-breach/

Hess, Eric (2015, June 24). *OPM: Data Breach II, Hearings before the Committee on Oversight and Government Reform, United States House of Representatives,* 114th Cong., Testimony of Eric Hess, CEO, KeyPoint Government Solutions on June 24, 2015. Retrieved from https://oversight.house.gov/hearing/opm-data-breach-part-i/

HIPPA Journal, (2015, Jul 5). *FBI Alert Suggests OPM/Anthem Malware Link.* Retrieved from http://www.hipaajournal.com/fbi-alert-suggests-opm-anthem-malware-link-8008/

Irvine, John J. (2015, June 15). *CyTech Services Confirms Assistance to OPM Breach Response*. Retrieved from http://www.prweb.com/releases/2015/06/prweb12787823.htm

Kadlec, John. (2015, August 5). *United Airlines Security Breach*. Retrieved from

https://www.watchpointdata.com/united-airlines-security-breach/

Kendall, Mary L. (2015, July 15). *Cybersecurity: The Department of the Interior, Hearings before the Committee on Oversight and Government Reform, Subcommittee on Information Technology and Subcommittee on Interior, United States House of Representatives,* 114th Cong., Testimony of Mary L. Kendall, Deputy Inspector General for the Department of the Interior on July 15, 2015. Retrieved from https://oversight.house.gov/hearing/cybersecurity-the-department-of-the-interior/

Krebs, B. (2015, February 9). *Anthem Breach May have Started in April 2014*. Retrieved from http://krebsonsecurity.com/2015/02/anthem-breach-may-have-started-in-april-2014/

Lyngass, Sean (2015, September 11). *OMB readies next phase of cyber sprint plan*. Retrieved from http://fcw.com/Articles/2015/09/11/OMB-post-cyber.aspx?p=1/

McFarland, Patrick E. (2015, June 24). *OPM: Data Breach II, Hearings before the Committee on Oversight and Government Reform, United States House of Representatives,* 114th Cong., Statement of the Honorable Patrick E. McFarland, Inspector General on June 24, 2015. Retrieved from https://oversight.house.gov/hearing/opm-data-breach-part-i/

Mazmanian, Adam (2015, July 15). *Interior IT flaws didn't lead to hack, says CIO*. Retrieved from http://fcw.com/articles/2015/07/15/house-ogr-on-interior-cyber.aspx

Miller, Jason (2015, June 17). OPM's Archaic Infrastructure Opened Door for Massive Data Breach. Retrieved from

http://federalnewsradio.com/congress/2015/06/opms-archaic-it-infrastructure-opened-door-for-massive-data-breach/

Office of Personnel Management (OPM) (2015), *Our People & Organization,* retrieved from https://www.opm.gov/about-us/

Office of Personnel Management (2015, June 29). *Actions to Strengthen Cybersecurity and Protect Critical IT Systems*. Retrieved from http://www.nage.org/news/OPM-Actions-to-Strengthen-Cybersecurity-and-Protect-Critical-IT-Systems.html

Office of Personnel Management, News Release (2015, July 13). *OPM Announces Steps to Protect Federal Workers and Others From Cyber Threats.* Retrieved from http://www.army.mil/article/152158/OPM_announces_steps_to_protect_federal_workers_and_others_from_cyber_threats/?from=RSS

Ozment, Andy (2015, June 16). *OPM: Data Breach, Hearings before the Committee on Oversight and Government Reform, United States House of Representatives*, 114th Cong., Testimony of Dr. Andy Ozment, Assistant Secretary for Cybersecurity and Communications, U.S. Department of Homeland Security on June 16, 2015. Retrieved from https://oversight.house.gov/hearing/opm-data-breach/

Paganini, Pierluigi (2012, March 8). *Cyberespionage and new opportunities for Cybercrime.* Retrieved from http://securityaffairs.co/wordpress/3158/cyber-crime/cyberespionage-and-new-opportunities-for-cybercrime.html

Pagliery, Jose (2015, July 10). *OPM hack's unprecedented haul: 1.1 million fingerprints*.

Retrieved from http://money.cnn.com/2015/07/10/technology/opm-hack-fingerprints/

Palmer, Danny. (2015, July 30). *United Airlines breached by Chinese hackers behind OPM cyber attack – report*. Retrieved from http://www.computing.co.uk/ctg/news/2420013/united-airlines-breached/

Peterson, Andrea (2015, June 15). *Data exposed in breaches can follow people forever. The protections offered in their wake don't*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2015/06/15/data/

Ragan, Steve (2015, June 30) FBI alert discloses malware tied to the OPM and Anthem attacks. Retrieved from http://www.csoonline.com/article/2942601/disaster-recovery/fbi-alert

Rashid, Fahmida Y. (2015, July 30). *United Airlines Hack Highlights Need for Improved Information Sharing*. Retrieved from http://www.securityweek.com/united-airlines-hack-highlights-need-improved-information-sharing

Riley, Charles (2015, February 4). *Insurance giant Anthem hit by massive data breach*. Retrieved from http://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/index.html

Riley, Michael & Robertson, Jordan (2015, July 29). *China-Tied Hackers That Hit U.S. Said to Breach United Airlines*. Retrieved from http://www.bloomberg.com/news/articles/2015-07-29/china-tied-hackers-that-hit-u-s-said-to-breach-united-airlines

Rouse, Margaret (2009). *RAT (remote access Trojan) definition*. Retrieved from http://searchsecurity.techtarget.com/definition/RAT-remote-access-Trojan

Philip G. Rynn, scholar59@hotmail.com

Sanger, David E. (2015, September 23). *Hackers Took Fingerprints of 5.6 Million U.S. Workers, Government Says.* Retrieved from http://www.nytimes.com/2015/09/24/world/asia/hackers-took-fingerprints-of-5-6-million-us-workers-government-says.html?_r=0

Scott, Tony (2015, June 16). *OPM: Data Breach, Hearings before the Committee on Oversight and Government Reform, United States House of Representatives*, 114th Cong., Testimony of Tony Scott, United States CIO, OMB on June 16, 2015. Retrieved from https://oversight.house.gov/hearing/opm-data-breach/

Secure Thoughts (2015). *The United Airlines Breach: Be Afraid.* Retrieved from http://securethoughts.com/the-united-airlines-breach-be-afraid/

Siciliano, Robert (2011, March 25). *Seven Types of Hacker Motivations*. Retrieved from www.infosecisland.com/blogview/12659-Seven-Types-of-Hacker-Motivations.html

Fields, Carlton, Seesel, Ben & Jorden, Burt (2015, September 3). *Cybersecurity as a Regulatory Issue: The NAIC Considers the Anthem Breach and Weighs a "Cybersecurity Bill of Rights".* Retrieved from http://www.jdsupra.com/legalnews/cybersecurity-as-a-regulatory-issue-the-71142/

Security Experts (2015, August 6). *Hackers Breach United Airlines*. Retrieved from http://www.informationsecuritybuzz.com/hackers-breach-united-airlines/

Threatconnect Intelligence Research Team (TCIRT) (2015, February 27). *The Anthem Hack: All Roads Lead to China:* Retrieved from http://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/

Philip G. Rynn, scholar59@hotmail.com

APPENDIX A
Selected Critical Security Controls for Implementation

Appendix A lists the specific Critical Security Controls and sub-controls that are recommended for implementation by United Airlines. These controls are extracted from *The Critical Security Controls for Effective Cyber Defense* (Version 5.0), as published by the Council on Cybersecurity.

CSC 5: Malware Defenses

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 actions.

- Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers (CSC 5-1).
- Employ anti-malware software that offers a remote, cloud-based centralized infrastructure that compiles information on file reputation or have administrators manually push updates to all machines. After applying an update, automated systems should verify that each system has received its signature update (CSC 5-2).
- Configure laptops, workstation, and servers so that they will not auto-run content from removable media, like USB tokens, USB hard drives, CD/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares (CSC 5-3).
- Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted (CSC 5-4).
- Scan and block all e-mail attachments entering e-mail gateway if they contain malicious code or file types that are unnecessary for business. This scanning should be done before the e-mail is placed in the user's

inbox. This includes e-mail content filtering and web-content filtering (CSC 5-5).

- Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased protection, deploy capabilities such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executables (CSC 5-6).
- Ensure that automated monitoring tools use behavior-based anomaly detection to complement traditional signature-based detection (CSC 5-8).
- Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint (CSC 5-9).
- Implement an incident response process that allows IT support organization to supply the security team with samples of malware running on corporate systems that do not appear to be recognized by the enterprise's anti-malware software. Samples should be provided to the security vendor for "out-of-band" signature creation and later deployed to the enterprise by system administrators (CSC 5-10).
- Enable domain name system (DNS) query logging to detect hostname lookup for known malicious C2 domains (CSC 5-11).

CSC 9: Security Skills Assessment and Appropriate Training to Fill Gaps

For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills and abilities needed to support defenses of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

- Perform gap analysis to see which skills employees need and which behaviors employees are not adhering to, using this information to build a baseline training and awareness roadmap for all employees (CSC 9-1).
- Deliver training to fill the skills gaps. If possible, use more senior staff to deliver the training. A second option is to have outside teachers provide training onsite so the examples used will be directly relevant (CSC 9-2).
- Implement an online security awareness program that (1) focuses only on the methods commonly used in intrusions that can be blocked through individual action, (2) is delivered in short, online modules convenient for employees, (3) is updated frequently (at least annually) to represent the latest attack techniques, (4) is mandated for completion by all employees at least annually, and (5) is reliably monitored for employee completion (CSC 9-3).
- Validate and improve awareness levels through periodic tests to see whether employees will click on a link from suspicious e-mail…; targeted training should be provided to those who fall victim to the exercise (CSC 9-4).
- Use security skills assessments for each of the mission-critical roles to identify skill gaps. Use hands-on, real-world examples to measure mastery. If you do not have such assessments, use one of the available online competitions that simulate real-world scenarios for each of the identified jobs in order to measure skill mastery (CSC 9-5).

CSC 17: Data Protection

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

- Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data (CSC 17-1).

Philip G. Rynn, scholar59@hotmail.com

- Verify that cryptographic devices and software are configured to use publicly-vetted algorithms (17-2).
- Perform an assessment of data to identify sensitive information that requires the application of encryption and integrity controls (CSC 17-3).
- Review cloud provider security practices for data protection" (17-4).
- Deploy an automated tool on network perimeters that monitors for certain sensitive information (PII), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel (CSC 17-5).
- Conduct periodic scans of server machines using automated tools to determine whether sensitive data (i.e. PII, health, credit card, and classified information) is present on the system in clear text. These tools, which search for patterns that indicate the presence of sensitive information, can help identify if a business or technical process is leaving behind or otherwise leaking information (CSC 17-6)
- Move data between networks using secure, authenticated, and encrypted mechanisms (CSC 17-7).
- If there is no business need for supporting such devices, configure systems so that they will not write data to USB tokens or USB hard drives. If such devices are required, enterprise software should be used that can configure systems to allow only specific USB devices (based on serial number or other unique property) to be accessed, and that can automatically encrypt all data placed on such devices. An inventory of all authorized devices must be maintained (CSC 17-8).
- Use network-based DLP [Data Loss Prevention] solutions to monitor and control the flow of data within the network. Any anomalies that exceed the normal traffic patterns should be noted and appropriate action taken to address them (CSC 17-9).

- Only allow approved Certificate Authorities (CAs) to issue certificates within the enterprise; Review and verify each CAs Certificate Practices Statement (CPS) and Certificate Policy (CP) (CSC 17-10).
- Perform an annual review of algorithms and key lengths in use for protection of sensitive data (CSC 17-11).
- Monitor all traffic leaving and detect any unauthorized use of encryption. Attackers often use an encrypted channel to bypass network security devices. Therefore it is essential that be able to detect rogue connections, terminate the connection, and remediate the infected system (CSC 17-12).
- Define roles and responsibilities related to management of encryption keys within the enterprise; define processes for lifecycle (CSC 17-14).
- Where applicable, implement Hardware Security Modules (HSMs) for protection of private keys (e.g. for sub CAs) or Key Encryption Keys (CSC 17-15).

APPENDIX B
CSC 5 – Malware Defenses
Automation & Effectiveness Metrics & Effectiveness Testing

Appendix B lists suggested effectiveness and automation metrics, and effectiveness testing, for the implementation of Malware Defense sub-controls at United Airlines. These recommended actions are compiled from *The Critical Security Controls for Effective Cyber Defense* (Version 5.0), as published by the Council on Cybersecurity.

Automation Metrics

1. How many instances of malicious code have been detected within a period of time by host-based anti-malware systems (by business unit)?
2. How many instances of malicious code that were detected within a period of time were automatically remediated by the organization's host-based anti-malware systems (by business unit)?
3. How many instances of malicious code have been detected within a period of time by network-based anti-malware systems (by business unit)?
4. How many instances of malicious code that were detected within a period of time were automatically remediated by the organization's network-based anti-malware systems (by business unit)?
5. Percentage of applications on a system that are not utilizing application sandboxing products (by business unit)?
6. Percentage of systems with anti-malware systems deployed, enabled and up-to-date (by business unit)?

Philip G. Rynn, scholar59@hotmail.com

Effectiveness Metrics

1. How long does it take the system to identify any malicious software that is installed, attempted to be installed, executed, or attempted to be executed on a computer system (time in minutes)?
2. How long does it take the system to send e-mail notification to a list of enterprise personnel via their centralized anti-malware console or event log system after malicious code has been identified (time in minutes)?
3. Does the system have the ability to block installation, prevent execution, or quarantine malicious software (yes or no)?
4. Does the system have the ability to identify the business unit in the organization where the malicious software was identified (yes or no)?
5. How long does it take the organization to completely remove the malicious code from the system after it has been identified (time in minutes)?

Effectiveness Test

1. Move a benign software test program appearing to be malware, but that is not included in an officially authorized software list, to 10 systems on the network via removable media. System selection must be as random as possible and include a cross-section of the organization's systems and location.
2. Verify that the systems generate an alert or e-mail notice regarding the benign malware within one hour.
3. Verify that the alert or e-mail indicating that the software has been quarantined or blocked is received within one hour.
4. Verify that the system provides details of the location of each machine with the test file, including information about the asset owner.
5. Verify that the benign file is blocked by attempting to execute or open it and verifying that it is not allowed to be accessed.
6. Repeat the test, but transfer the benign file to 10 systems via e-mail instead. The same notification results should occur via this mode of transmission.

Philip G. Rynn, scholar59@hotmail.com

APPENDIX C
CSC 9 – Security Skills Assessment and Appropriate Training to Fill Gaps Effectiveness Metrics

Appendix C lists suggested effectiveness metrics, for the implementation of Security Skills Assessment and Appropriate Training to Fill Gaps at United Airlines. These recommended metrics are compiled from *The Critical Security Controls for Effective Cyber Defense* (Version 5.0), as published by the Council on Cybersecurity.

Effectiveness Metrics

1. Participation rate for online training courses – percentage of staff completing security training (by business unit)?
2. Average scores of online tests, compared to baseline (previous tests, industry data if available, etc.) (by business unit)?
3. Average scores of periodic tests (e.g. click rates for test phishing emails) (by business unit)?
4. Individual scores on skill assessment tests for individual mission-critical roles (by business unit)?
5. Retention (or job opening fill rate) of mission critical roles (org/unit metric)?

Philip G. Rynn, scholar59@hotmail.com

APPENDIX D
CSC 17 – Data Protection
Automation & Effectiveness Metrics & Effectiveness Testing

Appendix D lists suggested effectiveness and automation metrics, and effectiveness testing, for the implementation of Data Protection sub-controls at United Airlines. These recommended actions are compiled from *The Critical Security Controls for Effective Cyber Defense* (Version 5.0), as published by the Council on Cybersecurity.

Automation Metrics

1. How many unauthorized data exfiltration attempts have been detected within a period of time by DLP (Data Loss Prevention) software?
2. How many plaintext instances of sensitive data have been detected within a period by automated scanning software?
3. How many attempts to access known file transfer and e-mail exfiltration websites have been detected within a period of time?

Effectiveness Metrics

1. Does the system and report on unauthorized data being exfiltrated, whether via network file transfers or removable media?
2. Does the system identify the attachment of unencrypted USB tokens and require encryption of tokens?
3. Does the system store cryptographic key material securely?
4. Does the system use only NIST-approved encryption algorithms?
5. Within one hour of a data exfiltration event or attempt, enterprise administrative personnel must be alerted by the appropriate monitoring system (yes/no).
6. Do alerts notifying of data exfiltration also note the system and location where the event or attempt occurred?
7. Are the systems able to identify the location, department, and other critical details about where the sensitive data originated from (yes/no)?
8. How long does it take before a data leakage risk has been remediated from the time that it was detected (time in minutes)?

Philip G. Rynn, scholar59@hotmail.com

Effectiveness Test

Evaluation must attempt to move test data sets that trigger DLP systems but do not contain sensitive data outside of the trusted computing environment via both network file transfers and removable media. Each of the following tests must be performed at least three (3) times:

1. Attempt to transfer large data sets across network boundaries from an internal system.
2. Attempt to transfer plaintext test data sets of personally identifiable information (that trigger DLP systems but that do not contain sensitive data) across network boundaries from an internal system (using multiple keywords specific to the business).
3. Attempt to transfer encrypted test data sets across network boundaries from an internal system to identify if the exfiltration is reported.
4. Attempt to maintain a persistent network connection for at least 10 hours across network boundaries between an internal and external system, even though little data may be exchanged.
5. Attempt to maintain a network connection across network boundaries using an anomalous service port number between an internal and external system.
6. Insert a USB token into an organization system and attempt to transfer example test data to the USB device.

Each test must be performed from multiple, widely-distributed systems on the organization's network in order to test the effectiveness of the monitoring systems. Once each of these events has occurred, the time that it takes for enterprise staff to respond to the event must be recorded.