Global Information Assurance Certification Paper

Securing Against the Most Common Vectors of Cyber Attacks

GIAC (GCCC) Gold Certification

Author: Richard Hummel, rhummel@mastersprogram.sans.edu
Advisor: Tanya Baccam
Accepted: August 2017

Final Version July 2017

Abstract

Advanced Persistent Threat (APT) adversaries run highly targeted, multifaceted campaigns to exploit vulnerabilities either through holes in an organization's security implementation or by targeting the human element which often uses social engineering. Financially motivated actors indiscriminately send mass spam emails in credential harvesting campaigns or deploy ransomware. These attack vectors are the most common against organizations of any size, but often have a greater impact on small to medium-sized business that may not have a robust security posture. As a security practitioner, it is imperative to posture an organization to prevent and mitigate the risk posed by these attacks. The Critical Security Controls (CSC) is the industry standard for securing an environment but may be costly and time-consuming to implement; also, some of them may not be as applicable to all organizations. In this study, the controls for Email and Web Browser Protection (#7) and Security Skills Assessment and Appropriate Training to Fill Gaps (CSC #17) are examined to secure against threats seeking to take advantage of end users, the most common entry point for an attacker. This paper examines multiple real-world threats and how the CSCs can be applied to prevent compromises. The goal of this research is to inform and educate security practitioners at any stage of the business on best practices and to aid in implementing controls directly applicable to their end users.

1. Introduction

Today is the time to hit the refresh button, take a step back, and evaluate what security practices are being leveraged to defend against APT and financially motivated attacks across the globe. As the year's progress, the cyber landscape remains in a constant battle of attack and defend. Unfortunately, the attacker holds the advantage with dozens, if not, hundreds, of different ways in which an organization is susceptible to attack. The defender has the overwhelming goal of defending the entire technology stack and plugging any hole in the security of an organization, which is nigh impossible with the slew of zero-days lacking secure coding practices. Notably, one of the greatest strengths and weaknesses to an organization's security posture is the human element. An employee properly educated in cyber-attacks and suitably restricted from critical systems can be a tremendous asset to the defense posture of an organization, often recognizing and reporting attempted attacks before any damage occurs. Contrast that to untrained individuals that will immediately click a malicious URL, browse to suspicious web sites, or enable that script to run in a weaponized document. Attackers are well-aware that humans are susceptible to these types of attacks and as before-mentioned, it continues to be the number one initial vector for intrusions.

Recognizing that emails are the most common intrusion vector; security practitioners can safely assume it is high time to step up and take proactive steps to defend this threat. Although there are many ways in which an organization can take measures to secure against this vector, the Center for Internet Security (CIS) offers twenty highly effective and widely accepted recommendations called the Critical Security Controls (CSC). These controls act in order of significance but often are not practical for businesses that may not have the required or necessary budget. The controls offer a top-down approach to a layered defense or defense-in-depth. As such, many of the controls overlap to some degree. By analyzing these overlapping controls, organizations can create minimal baseline security postures, while saving the overhead costs. They can then implement the full controls over time. If budget and time constraints are a pressing issue, organizations can narrow the scope of implementation for the controls and focus on email and web-based attacks as these are the most comment vector used by attackers. Addressing these

Author Name, email@address

common attack points allows for faster implementation of security that may act as the first line of defense against an adversary.

2. Evaluating the Threat Landscape

Commercial, government, nonprofit organizations around the world experience data breaches from state-sponsored (espionage) cyber operators as well as financially motivated actors looking to exploit data obtained during an attack. A large percentage of these attacks use widely known methods to commit cyber-attacks. However, even knowing these common methods, there are many other aspects associated with a malicious cyber operation to consider. Verizon, in their Data Breach Digest, notes that "data breaches are involved affairs often using some combination of human factors, hardware devices, exploited configurations or malicious software. As can be expected, data breach response activities—investigation, containment, eradication, notification, and recovery—are proportionately complex." (Verizon, 2017). Tactics, techniques, and procedures (TTP) leveraged by attackers are abundant and ever-evolving, and it can be difficult to defend against all threats. Throughout the past few years, major organizations like Verizon and FireEye (Mandiant) release year-in-review reports such as the DBIR or M-Trends. These reports detail threats posed across the world, including the TTP's attacker's use to gain an initial foothold. In most scenarios over the past few years, e-mail has been the most common way in which an attacker gains access, followed by web-based attacks often occurring in the form of drive-by attacks featuring an Exploit Kit. Because these attacks are always evolving, security practitioners should be aware of these year-in-review reports from well-established security-oriented organizations to stay informed of the current threat landscape.

In researching the threat landscape, security practitioners can evaluate what threats are active in their region, interests, and verticals. Identifying who might be attacking and how the attacks occur then enable an organization to set in motion a security policy that first mitigates the threats targeting them and, in time, sets up a more robust, layered defense. Verizon states, “Knowing which incident patterns affect your industry more often than others do provides a building block for allocating cyber security resources”

(Verizon, 2017). Symantec analyst Candid Wueest, in the *Internet Security Threat Report Financial Threats Review 2017*, also agrees with Verizon's assessment regarding knowing which threats and incidents affect a given organization and he takes it a step further by outlining the "weapon of choice" used by cyber adversaries:

> Malicious emails were the weapon of choice for a wide range of cyber-attacks during 2016, used by everyone from state sponsored cyber espionage groups to mass-mailing ransomware gangs. One in 131 emails sent were malicious, the highest rate in five years. Email's renewed popularity has been driven by several factors. It is a proven attack channel. It doesn't rely on vulnerabilities, but instead uses simple deception to lure victims into opening attachments, following links, or disclosing their credentials. Spear-phishing emails, such as spoofed emails instructing targets to reset their Gmail password, were used in the US election attacks. Malicious emails disguised as routine correspondence, such as invoices or delivery notifications, were meanwhile the favored means of spreading ransomware. The availability of spam botnets-for-hire, such as Necurs, allowed ransomware groups to mount massive email campaigns during 2016, pumping out hundreds of thousands of malicious emails daily. (Wueest, 2017)

As Wueest points out in the ISTR, email is often the chosen method of delivering threats to victims because it is trivial, successful, and has been a time-proven method for many years. In previous years, email and web browsers often ebb and flow for the top contender as the most common attack vector, but in most recent years, email wins the top spot, often followed by web browser attacks. Symantec noted the number of critical attacks in which browsers were the initial vector has diminished by 6% over the last year, but they continue to be a popular interest among attackers as Symantec also notes that 76% of scanned web sites contained vulnerabilities. Notably, this is only a 2% decrease from previous years. (Wueest, 2017). Given two different perspectives, Verizon and Symantec, who have vast insight into the victim environment, it is safe to assume that email and web browser attacks are the most distinguished method used by cyber adversaries. Email and web browsers, these two common attack vectors, comprise a vast array of the threat landscape and should be the focus of organizations looking to establish a quick and effective defense against attackers. Because it is the most common form of

attack, it makes the most sense from a risk to business and cost perspective to focus on these two areas before embarking on a multi-year security policy implementation.

2.1. Examining the Most Common Initial Intrusion Vector

As previously noted by Wueest in the Symantec ISTR, email continues to be the most common factor related to intrusions in any organization. Verizon further states that "across industries, email is the road most traveled to deliver malware into organizations. The vectors of mail and web browser are further broken down into malware packaged in an Office document, an executable application, or 'Other'." (Verizon, 2017). It could be further broken down into types of office documents, what script languages are used, or are there any weaponized documents using zero-day vulnerabilities. In addition to the various ways in which adversaries distribute malware, Wueest says "just over half (53%) of all emails are spam…[and] malware authors can outsource their spamming operations to specialized groups who conduct major spam operations." (Wueest, 2017) Again, the pervasiveness of email threats highlights the need for organizations to get serious and pay attention to protect and defend against cyber adversaries

Understanding external threats requires inside knowledge of the attack surface, visibility into victims that have been impacted by external threats. Verizon has a very advantageous position that allows them to see the attack surface in many different industries and verticals as such can divulge statistics that show real-world threats as they occur. According to Verizon, "There were a little over 1,600 incidents and more than 800 breaches featuring social actions in this year's corpus (all external actor driven). Phishing was again the top variety, found in over 90% of both incidents and breaches." (Verizon, 2017) One of the methods that an attacker will employ is including links to phishing pages or other malicious web sites in spam emails. These will often be disguised hyperlinks to other legitimate websites, but when clicked are redirections to the phishing site. An analyst, Greg Aaron, in association with the Anti-Phishing Working Group (APWG) notes in Figure 1 that from October 2015 to March 2016, phishing sites increased 250%.

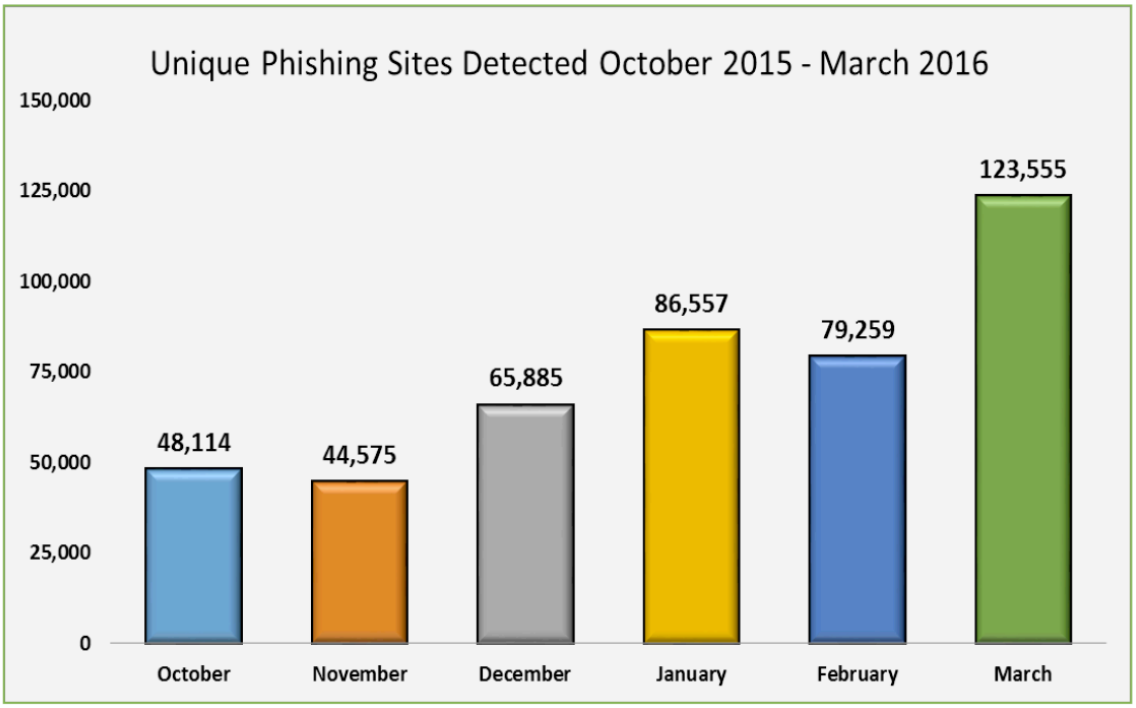

Figure 1: Unique Phishing Sites Detected October 2015 – March 2016 (Aaron, 2016)

Although these phishing site numbers are from October of 2016, the numbers continue to increase, and the evidence portrayed by both Verizon and Symantec of the continued increase in spam email provide ample evidence of this trend. The facts are undisputed, the email vector, whether this uses attachments, documents, scripts, or malicious URLs, accounts for the largest number of attacks and attacks leading to successful intrusions. Therefore, it is imperative that organizations take this risk seriously and immediately take steps to defend against it.

2.2. Threat Actors Targeting the Human Element

Looking at the human element in the attacker's methodology allows security professionals to understand why email and web browsers are the primary intrusion vector. As explained in the Verizon DBIR, "Eagerness. Distraction. Curiosity. Uncertainty. These are drivers of human behavior, and one or more can be leveraged to influence someone to disclose information, click a link or wire money to a "vendor" account." (Verizon, 2017) According to Verizon, 98% of attacks leveraging social engineering came in the form of phishing emails. (Verizon, 2017) There are many factors

to evaluate when considering human behavior and how it impacts the bottom line of a security posture for any organization. Some of these areas to evaluate include, but are not limited to the following:

1. Education (both professionally and as it relates to cyber awareness)
2. Experience in the workforce.
3. Local security policy on the employee's machine.
    a. Is the machine running with local administration privilege?
    b. Are there restrictions for application installation by the user?
    c. Are scripts able to be executed from the browser on sites an employee visits?
    d. Can the user enable scripts and macros in documents?
4. What applications are enabled on systems the user has access to?

While it is true that the human element is the most common vector for an attacker, there are many areas outside the control of the typical end-user that may contribute to the problem, such as those mentioned in the list above. An educated or trained end-user is an asset to any organization when he or she takes proactive steps to alert security personnel to attempted phishing emails or if the user begins noticing unusual behavior after visiting a web site. How an organization can help users and shore up defenses for these areas will be examined in greater detail using the Critical Security Controls below.

3. Lessons Learned

Interviewing security experts around the globe can provide insight into the lifecycle of an incident. Due to the sensitivity associated with breach investigations and intrusions, many of the security experts interviewed wish to remain anonymous, but have been willing participants to share knowledge with the rest of the community. To achieve a baseline, several interviews were conducted using the same list of questions. Each participant was asked to provide a response to these topics while ensuring sanitization of anything sensitive. One security expert, Ruchir Arya, a cyber security analyst with the New Jersey Institute of Technology, comes from the unique perspective of having been

involved in incidents impacting a variety of organizations in multiple industries and regions. The following incidents and organizational data shared are fully anonymized so as to protect all parties involved. Charts 1 – 3 below highlight the interview questions and the responses given for each incident. These interview questions and answers highlight the need to have a security posture in place to aid in defense against email and web browser based attacks.

3.1. Breached Organization Baseline

The first chart, **Chart 1: Organization**, is necessary to establish a baseline of the entities involved. Initially, this process had started out with small to medium sized organizations. As participants responded to the interview questions, it was readily apparent that regardless of the size of the organization, the same problems existed across the dataset as noted by a difference of approximately 80,000 employees from one incident to the next. The problem is also not limited by industry and region. The first column indicates the context of the questions asked to each interviewee and columns 1-3 the answers from each respondent.

Chart 1: Organization

	Company #1	Company #2	Company #3
Industry	Energy	Manufacturing	Health Care
Region	North America	Germany	Non-Specified
Size	20k	100k	25k
Security Team	30	20	N/A
Security Framework	None	Unknown	Unknown
Cyber Awareness Program	• Phishme • Occasional security presentation	• Unknown program in place	• Unknown program in place
Damages	• Monetary losses in the millions	• Proprietary data loss • Operation impact during Incident Response	• PII theft • Reputation damage • Operational impact during remediation

Policy Response	• Security Process Reform	• Increased security team size • Proposal for more secure architecture • Adoption of new technologies	• Better Incident Response procedures • Inclusion of better forensic tools for incident responders • Whitelisting • Cyber awareness program improvement • Periodic penetration testing

3.2. Incident Response from Breached Organizations

In addition to providing a baseline for their respective organizations or those organizations those interviewed previously worked for, the interviewees provided insight into the incident including initial entry, remediation steps, and preventative measures put in place following the incident. The first column of **Chart 2: Incident Details** indicates the context of the questions asked to each interviewee and columns 1-3 the answers from each respondent.

Chart 2: Incident Details

	Company #1	Company #2	Company #3
Initial Access	• Emails	• Phishing emails (credential theft and delivering payloads to open a backdoor)	• Email (ZIP with embedded script) • Web Browser (.js, .swf, .hta. Ps1, .wsf files)
Initial Payload	• Unknown	• Unknown	• Varied
Lateral Movement	• No lateral movement observed	• Psexec • Mimikatz • RDP • Network shares movement	• Domain Controllers, • Psexec • Powershell • Wmic
Data Targeted	• Access to business	• No known focus	• SSN • User credentials

Author Name, email@address

	accounts for fraud		• Network architecture
Company Loss	• Monetary losses (funds unrecoverable)	• Unknown data theft • Long term monetary loss due to operational disruption	• Exfiltrated PII • Proprietary information loss
Remediation Steps	• N/A	• System-by-System cleanup • System baselining	• Re-baseline endpoints • Restore from secure backups • Use whitelisting for applications
Preventative Measures Established	• No steps taken (considered email security tools)	• Additional logging • Technology updates	• Host-Intrusion Prevention (HIP) using behavior-based detection
Motivation Behind Attack	• Fraud	• Unknown	• Minimal targeted intrusions • Most attacks appeared to be random

In every instance of a breach listed above, the losses to the organizations include significant monetary loss, data theft, and personally identifiable information (PII) theft. In all three of these instances, email or web browsers were used as the initial entry point, further highlighting the need for organizations to take immediate and proactive steps to counter these two avenues of attack. Because email continues to be the primary method of attack, defenders can focus and give priority to defending that attack vector first, followed by web browser based attacks.

3.3. Aftermath of a Breached Organization

The region, size, and industry of an organization are important factors to consider in a security investigation, but the reality is that every single organization, small, medium, and large experience the same types of threats and can take the same steps to begin protecting their company. To that end, the security experts interviewed came from many

different sizes, geographically diverse, and organizations spread across multiple industries. The reality of the answers for all of the interviewed experts highlights specific areas to focus on such as workforce education, more robust incident response procedures, or overhauling company policy. **Chart 3: Aftermath** goes through five questions, the context of which is provided in column 1, to ascertain what took place following a breach investigation and further to provide some advice to other security experts in the field.

	Company #1	Company #2	Company #3
Risk Prevention	• Train staff to recognize phishing	• Properly patching systems • Better logging to detect attacks and lateral movement	• Proper Incident response in place would have mitigated the bulk of the damages
Lessons Learned	• N/A	• Immediate connection with security experts • Connect with security teams from companies in the same sector	• Incident Response changes
Recommended Practices	• N/A	• More resources are required to suitably respond to incidents (this is likely related to personnel increase, but could likely be software/hardware as well)	• Provide minimal privilege to employees • Application whitelisting • Limited ability to execute scripts by users • Trust only digitally signed applications
Cleanup Length	• 6mo. - 1yr.	• Several Months.	• Several months
Takeaway's	• Secure the people: give the tools, information, and training needed to recognize and mitigate an attack	• Share experiences and knowledge with the community • Build trusted relationships with other teams	• N/A

Author Name, email@address

The responses from correspondents such as "Secure the people" and "share knowledge and build trust" provide sound advice and is the primary focus of this report, which is to give security experts around the world with the insight needed to begin working on protecting their organization and to "secure the people." Defending against email and web browser attacks can often be as easy as properly educating an organization's workforce so that they are aware of how an attack might look. While this will not fix all security gaps for a company, it is an efficient place to begin alongside working towards the technical implications of securing email and web browsers from attacks.

4. CSC #7: Email and Web Browser Protections

To “minimize the attack surface” defenders must address gaps in security mechanisms and policy in place for their respective organizations. The CIS, in the *Critical Security Controls,* instructs to “Minimize the attack surface and opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems” (CIS, 2016). In some of these instances, that means having a policy and defense, as many small to medium sized business do not even address the issue of security, falsely assuming they would never be the victim of an attack. The stark reality is that many cyber criminals (non-nation-state) often send spam emails indiscriminately and will take advantage of any situation given the opportunity resulting in every organization needing to defend against these adversaries.

In most instances of email being the initial vector of intrusion, the attacker will use social engineering to entice the user to open an email attachment, click a link, or enable script execution. Attackers have become very savvy at being persuasive and often rely on third- party spam message distributors who have had high success in compromising extensive quantities of users. Because this is one of the primary methods of entry, the CIS has continued to include CSC #7, although CSC # 1 to 6 also addresses security gaps that can enable defense from email and web browser attacks. Security experts in any industry and region will also conclude that control seven in dealing with

email and web browser security is necessary to include with specific instructions for defending against these threats.

4.1. How CSC #7 May Mitigate the Risk Posed to the Most Common Initial Entry Point

The CIS provides many sub-controls to protect against threats posed by email and web browsers. The first issue addressed will be email since often many of the web browser- related issues result in users clicking links in emails and being redirected to malicious web sites that may have an exploit kit (EK) installed. The following sub-controls address the issues of email security and provide a framework to defend; practical application for these sub-controls follows in the next section.

- 7.2 – "Uninstall or disable any unnecessary or unauthorized browser or email client plugins or add-on applications…" (CIS, 2016).
- 7.3 – "Limit the use of unnecessary scripting languages in all web browsers and email clients [JavaScript, Visual Basic Script, Macro-based Scripts] …" (CIS, 2016).
- 7.7 – "To lower the chance of spoofed email messages, implement the Sender Policy Framework (SPF) by deploying SPF records in DNS and enabling receiver-side verification in mail servers" (CIS, 2016).
- 7.8 – "Scan and block all email attachments entering the organization's email gateway if they contain malicious code or file types that are unnecessary for the organization's business. This scanning should be done before the email is placed in the user's inbox. This includes email content filtering and web content filtering" (CIS, 2016).

4.1.1. Sub-Control 7.2: Disable Add-ins, Plugins, or Extensions

With the vast number of email clients and web browsers likely in use within an organization, this practical application will focus on the most popular applications to include Microsoft Office (Excel, Word, Outlook), Firefox, Chrome, and Internet Explorer. Looking at the previous list of sub-controls and proceeding in order, the first step will be to disable plugins in email and web browsers. Rather than focusing on

individual accounts, the group policy or administrative template will be examined to enforce an organization-wide application of the recommendation.

Microsoft Outlook – To disable add-ins/plugins in Outlook 2013 and 2016, change the **List of managed add-ins** group policy setting. In addition to this main setting, group policy managers can also **Block all unmanaged add-ins**, as noted on the Microsoft website titled *No Add-ins loaded due to group policy settings for Office 2013 and Office 2016 programs*. (Microsoft, 2015) **Figure 2: Outlook Add-ins Group Policy Settings** shows the exact location as specified by Microsoft on their Technet website titled *Group Policy Administrative Template files (ADMX, ADML) and Office Customization Tool (OCT) files for Office 2013*. (Microsoft 2016) The Registry setting will be one of three values:

- 0: The add-in is always disabled (blocked)
- 1: The add-in is always enabled
- 2: The add-in can be manually enabled or disabled by the user

List of managed add-ins (Outlook)	**Group Policy location:** User Configuration\Administrative Templates\Microsoft Outlook 2013\Miscellaneous	**Group Policy registry path:** HKEY_CURRENT_USER\software\policies\microsoft\office\15.0\outlook\resiliency!addinlist	Allows you to specify which add-ins are always enabled, always disabled (blocked), or configurable by the user. To block add-ins that are not managed by this policy setting, you must also configure the **Block all unmanaged add-ins** policy setting.

Figure 2: Microsoft Outlook Add-in Group Policy Settings (Microsoft, 2016)

Microsoft Internet Explorer (IE) (v11) – The settings for IE11 are very similar to Microsoft Outlook (above) and are in the following object location:

- Computer Configuration\Administrative Templates\Windows Components\Internet Explorer

Once located, the setting or object has the following options available to group policy administrators as specified on the Microsoft website titled *Enable and disable add-ons using administrative templates and group policy (Internet Explorer 11 for IT Pros)*. (Microsoft, 2017):

1. Change any or all of these settings to match a company's policy and requirements.

- Turn off add-on performance notifications
- Automatically activate newly installed add-ons
- Do not allow users to enable or disable add-ons

2. Go into the **Internet Control Panel\Advance Page** folder, where it is possible to change the following:
    - Do not allow resetting IE settings
    - Allow third-party browser extensions
3. Go into the **Security Features\Add-on Management** folder, where it is possible to change the following:
    - Add-on List
    - Deny all add-ons unless specifically allowed in the Add-on List
    - Turn off Adobe Flash in IE and prevent applications from using IE technology to instantiate Flash objects (Microsoft, 2017)

Firefox Add-ons/Extensions – The Firefox add-on and group policy management requires additional software or an enterprise version of Firefox. Mark Sammons and Malte Schwarzkopf have created a version called *FirefoxADM* that provides group policy options. However, once implemented, Firefox will show up in the Group Policy Editor as noted on a Unidesk blog from Ron Oglesby, *How to Disable Firefox Auto Updates*, and portrayed in **Figure 3: Firefox Group Policy Settings Firefox Add-ins.**

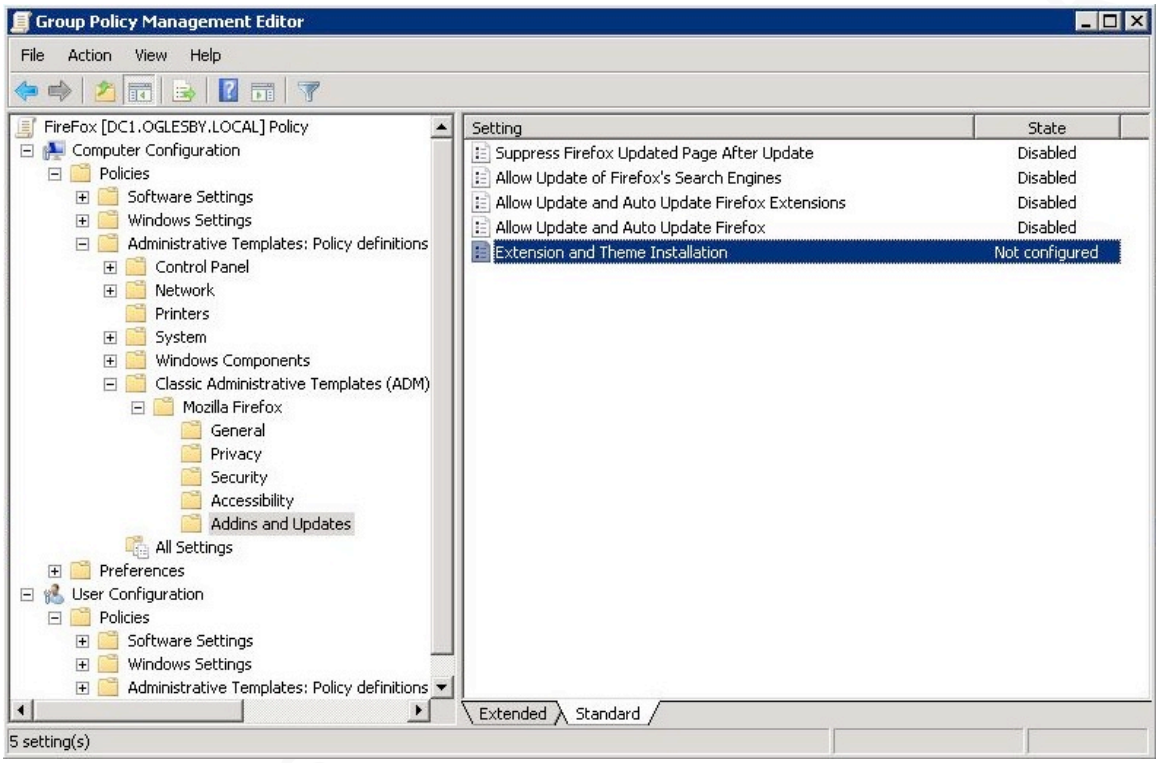

Figure 3: Firefox Group Policy Settings Firefox Add-ins (Oglesby, 2011)

Chrome Add-ons/Extensions – Looking at the source code and settings on *The Chromium Project* web site titled "Policy List," Chrome many of different settings that can be set regarding extensions to include the following list:

- **ExtensionInstallBlacklist:**
  - Specify which extensions a user cannot install.
- **ExtensionInstallWhitelist:**
  - By default, all extensions are white-listed, but all extensions can be black-listed using an asterisk (*) and then the white-list used to define which extensions are allowed.
- **ExtensionInstallForcelist:**
  - Specify a list of applications that install silently, without user interaction, and which cannot be uninstalled or disabled by the user.
- **ExtensionInstallSources:**
  - Specify which URLs can install extensions.
- **ExtensionAllowedTypes:**

Author Name, email@address

- Specify which extension types can be installed and limit runtime. (the Chromium Project)

Figure 4: Group Policy Settings Chrome Extensions, shows an example, from the *Group Policy Administrative Templates* website article titled *Configure extension, app, and user script install sources*, of allowing extensions/scripts from approved sources from a Group Policy perspective.

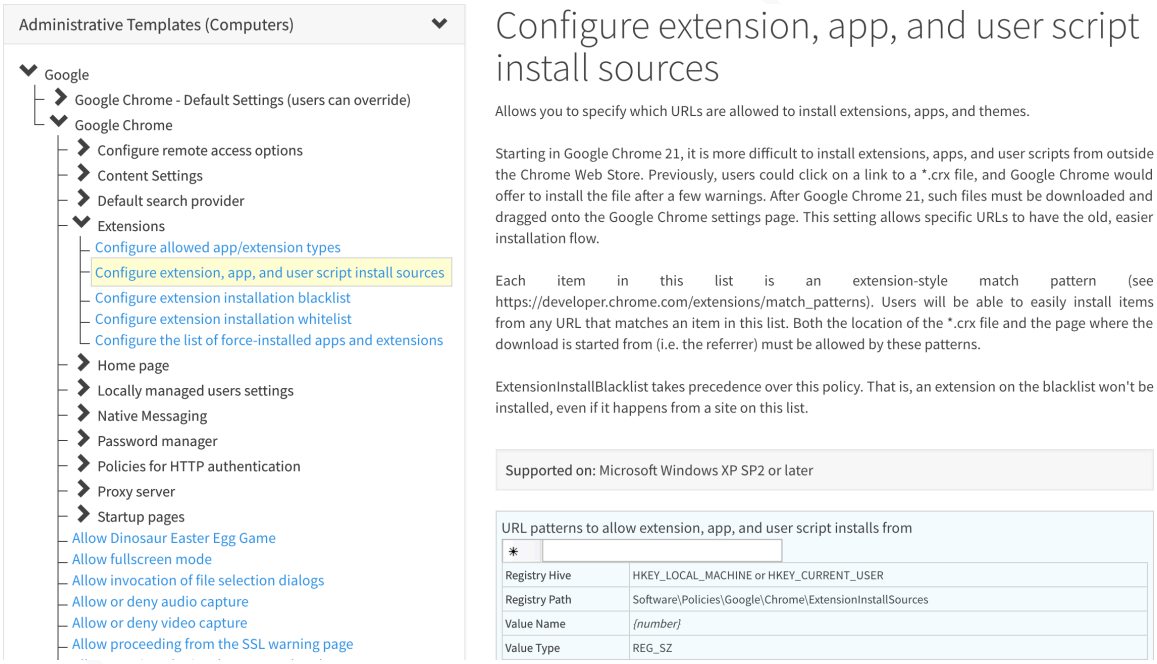

Figure 4: Group Policy Settings Chrome Extensions (Group Policy Administrative Templates)

4.1.2. Sub-Control 7.3: Disable Scripting Languages

Many web browsers require scripts such as JavaScript and Flash enabled for some websites to render appropriately and display content. However, this also leaves the user open to exploitation when visiting a malicious website. According to Symantec's Wueest, "Office macro downloaders (W97M.Downloader and variants) and JavaScript downloaders (JS.Downloader and variants) are the most commonly used downloaders that spread malware via email" (Wueest, 2017). There are several recommendations based on these findings such as allowing only scripts to run on approved websites or disabling scripting languages altogether. The same is true of applications like Microsoft Office. For instance, Office 2016 and Office 365 allow for group policy settings that will disable macros/scripts from running for all users or just specific users and can specify to block macros originating from the Internet.

Author Name, email@address

Internet Explorer Script Disable - The Internet Explorer settings to enable/disable scripting is the same as addressed in the "add-ins" section above. By disabling add-ins, JavaScript and VBScripts are also disabled and require explicit instructions to allow execution.

Firefox Script Disable – As with disabling add-ins/extensions, Firefox requires the installation of a supported Enterprise version or addition of a GPO extension in the browser to change the following script settings, such as *FirefoxADM*. (Schwarzkopf & Sammons, 2013):

- POLICY "Disable Java"
  - VALUENAME FirefoxJavaState
  - VALUEON NUMERIC 0 (disables Java)
  - VALUEOFF NUMERIC 1 (enables Java)

- POLICY "Disable JavaScript"
  - VALUENAME FirefoxJavascriptState
  - VALUEON NUMERIC 0 (disables JavaScript)
  - VALUEOFF NUMERIC 1 (enables JavaScript)

Chrome Script Disable – Chrome will also require a group policy and Active Directory template like Firefox to disable JavaScript/Java in web browsers. Many of the templates can be downloaded directly from Google, Mozilla, Microsoft (for each respective browser). Additionally, settings for these templates (ADM files) are located on the getadmx.com web site. **Figure 5: Group Policy Settings Chrome JavaScript** (below) is from the *Group Policy Administrative Templates* website titled *Configure extension, app, and user script install sources* and shows the options for enabling or disabling JavaScript. (Group Policy Administrative Templates)

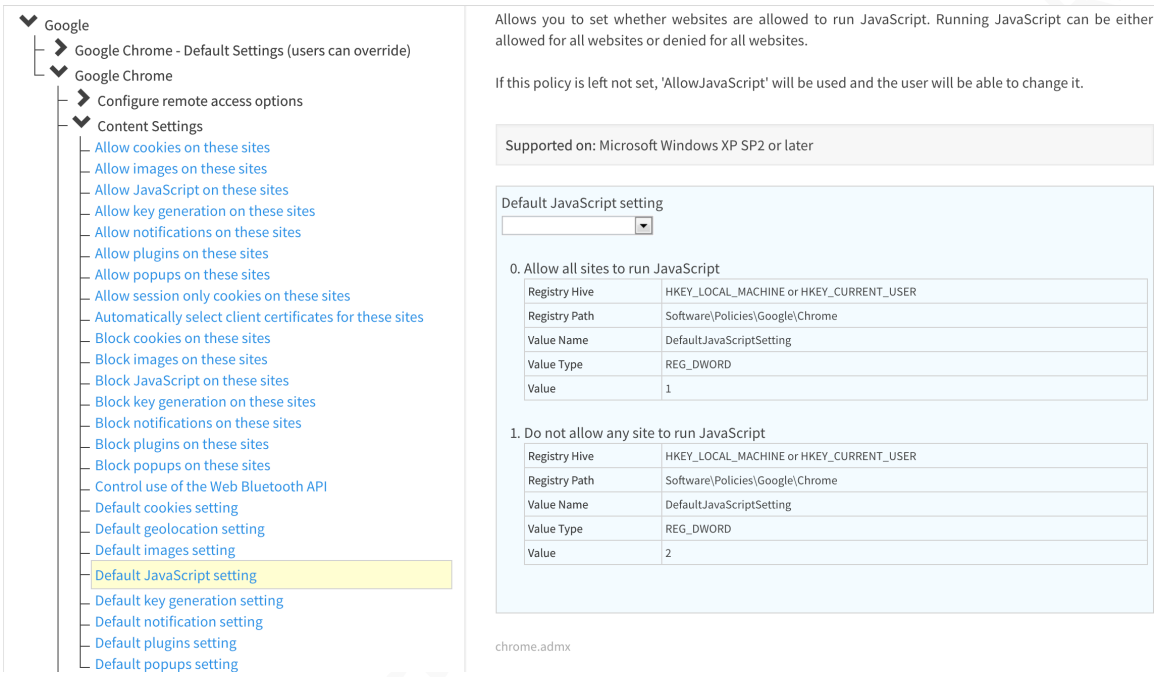

Figure 5: Group Policy Settings Chrome JavaScript (Group Policy Administrative Templates)

Microsoft Office Script and Macro Disable – In addition to web browser based scripts, email based threats can also use scripts. These threats often come in the form of a malicious macro, but can also use scripts such JavaScript and VBScript executed in a document (xls, word, ppt, etc.). Disabling macros and scripts for Office documents requires multiple steps. The first step addressed is that of disabling Visual Basic (VB) scripts in applications as seen in **Figure 6: Group Policy Settings Microsoft Office VBA** on the *Group Policy Administrative Templates* website titled "Disable VBA for Office applications."

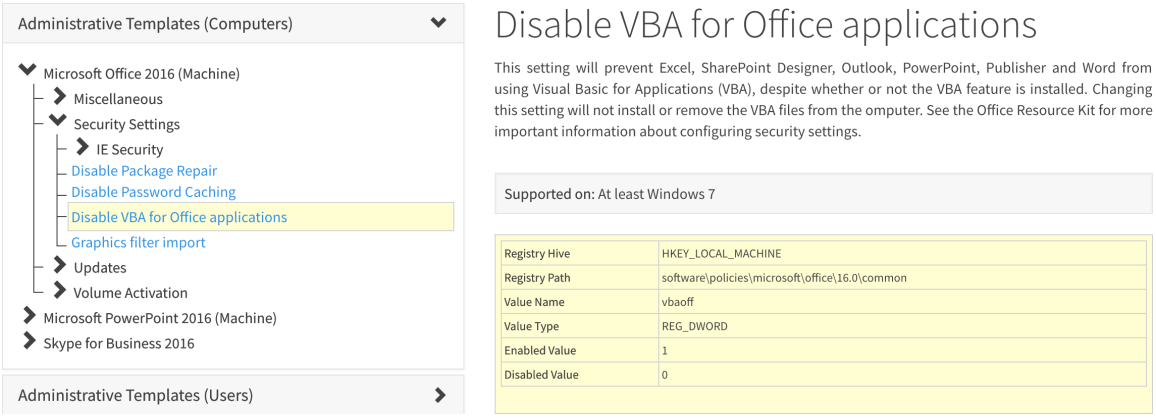

Figure 6: Group Policy Settings Microsoft Office VBA (Group Policy Administrative Templates)

Author Name, email@address

Most of the JavaScript and VBScripts used to infect via email come in the form of Macros within a document that requires users to "enable content" to execute. Microsoft has realized that organizations need the ability to block macros, especially macros that come from Internet sources as this is the way attacker often get malicious macros into an organization. **Figure 7: Group Policy Settings Microsoft Office Macros,** *Group Policy Administrative Templates* website titled *Block macros from running in Office files from the Internet*, shows the template settings used to disallow macros when the Office file came from the Internet:

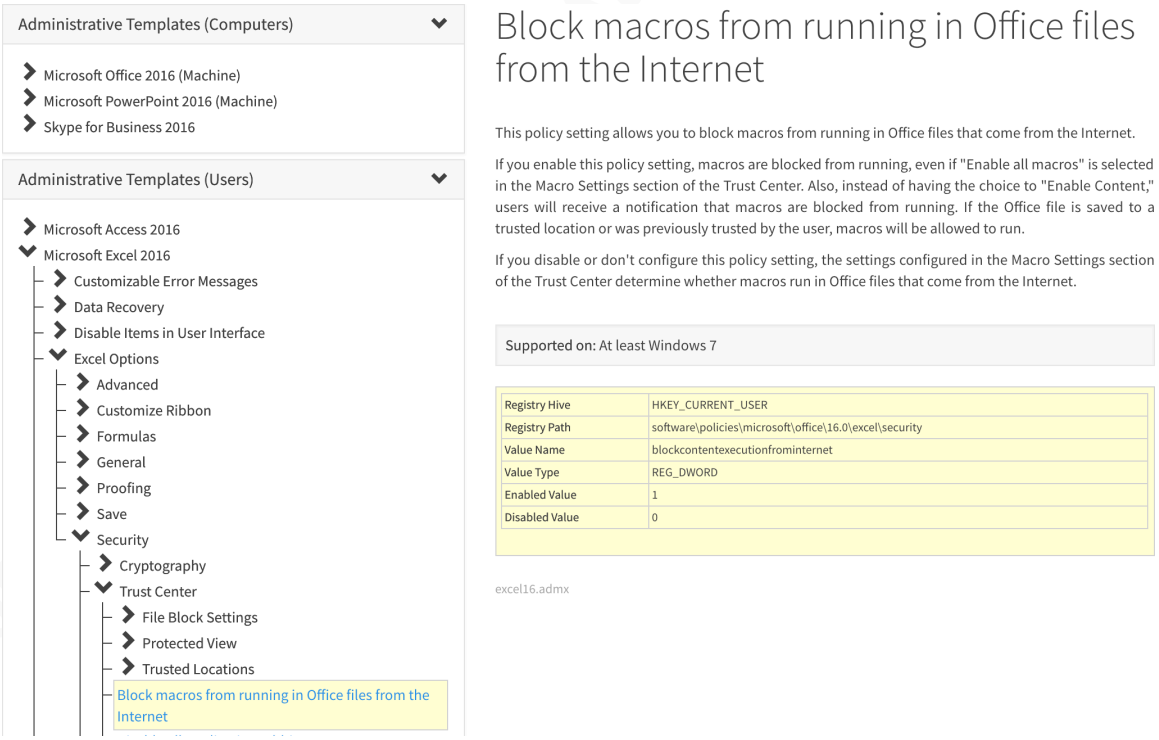

Figure 7: Group Policy Settings Microsoft Office Macros (Group Policy Administrative Templates)

In addition to disallowing just macros from files on the Internet, Microsoft allows the group policy editor to set Macro warning levels using the following settings:

- Always warn of Macro content
- Never warn, disable all content
- Warn for signed macros and disable unsigned
- No security check

All the methods for preventing script and macro execution on victim machines are a sure step in securing an organization against, what many security companies call, the

number one threat and entry point for an attacker. Depending on the setup of an organization, it may require one or all of the above steps to ensure coverage on all potential infection vectors. There are also many other web browsers and email clients not reported in this study, and each will require security practitioners to conduct additional research to determine how to secure against email and web-browser based threats.

4.1.3. Sub-Control 7.7: Implement Send Policy Framework (SPF)

The SPF is used to verify that outbound email from an organizations' domain is legitimate. Enabling SPF will be different for many organizations depending on hosting providers or email clients. Microsoft Office 365 usage is broad and represents a baseline case study for this research. Several steps, noted on Microsoft's Technet web site titled *Set up SPF in Office 365 to help prevent spoofing*, need to be taken to create an SPF record and prevent unauthorized messages.

1. Create a TXT record for SPF
    a. This step will vary depending on DNS provider
2. Enumerate a list of all IP addresses used for mail servers in the organization and include any third- party domains used for messaging.
3. Choose the syntax or enforcement rule for the SPF from the following three options:
    a. –all: Hard Fail, will drop any messages not from specified IPs or domains.
    b. ~all: Soft Fail, this is used if not all IPs or domains are known and included in the SPF record to mitigate legitimate email from being dropped.
    c. ?all: Neutral, often used in testing and not recommended for production environments. (Microsoft, 2016)

In addition to creating an SPF record, organizations may also create "DomainKeys Identified Mail (DKIM) with Office 365" in order to prevent attackers from spoofing emails that appear to be originating from the organization's domain. (Microsoft, 2017)

The last recommended step in this category is Domain-Based Message Authentication, Reporting, and Conformance (DMARC). This step, explained on

Microsoft's Technet web site titled *Use DMARC to validate email in Office 365*, is recommended last as it works with both the SPF and DKIM to verify the sender and ensure destination mail servers trust the originating domain. (Microsoft, 2016)

4.1.4. Sub-Control 7.8: Scan and Block Malicious Emails/Email Attachments

Although many organizations already have services in place to scan and block malicious emails and attachments, there are hundreds of email filtering/scanning services that organizations can implement. Some organizations may employ "on-premise" solutions such as appliances, but cloud-based solutions may be easier and faster to achieve for most organizations since there is virtually no overhead for the organization and it is simply a matter of altering the direction of email traffic to a different address. The following is a list of service providers for email-based security that has positive reviews.

- FireEye ETP
- Cisco Email Security
- Symantec Email Security.cloud
- Sophos Email

In most of the services listed above, the service works by altering the Mail Exchange (MX) record for mail servers used by the organizations. After the MX record is modified to redirect through the purchased service, many useful options are available, including full scanning of emails, URLs, and attachments; alerting on any suspected malicious behavior; blocking of known or suspected threats; passive examination of emails and logging. For instance, the FireEye ETP, outlined on the website titled Cloud Email Security Datasheet, is a solution that will examine all incoming mail, run any attachments, URLs, files through their Multi-Vector Virtual Execution System (MVX). MVX is then able to determine if any emails lead to malicious URLs or have attachments containing malware or scripts that will execute threats on the victim's machine.

In addition to the paid for services, Microsoft also offers a variety of services with Office 365 and GPO's. Many of these options are already included in previous sections,

but there are additional options that will prevent hyperlinks for suspected malicious URLs in emails among other GPO settings that will allow security personnel to create rules for filtering without the inclusion of a third-party service. Regardless of which option used, it is vital that email security is put into action considering it is the primary method of entry for most attacks that may result in a breach.

4.2. CSC # 17: Security Skills Assessment and Appropriate Training to Fill Gaps

After addressing the technical gaps in security, the human element must become the primary focus as it is the primary target an attacker uses to leverage the technical gaps previously discussed. Attackers rely on social-engineering to achieve arbitrary code execution on victim machines. Many APT actors will use weaponized documents that leverage exploits and 0-day vulnerabilities that do not require user interaction, but the larger portion of attacks require user interaction and confirmation to execute on the victim machine. According to Verizon,

> Our non-incident phishing data is comprised of 7.3 million records (campaign data down to user level), over 14,000 campaigns, and over three million unique users across 2,280 different organizations…. 7.3% of users across multiple data contributors were successfully phished—whether via a link or an opened attachment. That begged the question, 'How many users fell victim more than once over the course of a year?' The answer is, in a typical company (with 30 or more employees), about 15% of all unique users who fell victim once, also took the bait a second time. 3% of all unique users clicked more than twice, and finally less than 1% clicked more than three times. (Verizon, 2017)

This statement highlights the importance of having some form of education and cyber awareness campaign in every organization that will educate their employee base to recognize and report potential threats. The primary recommendation for "Securing the Human" as SANS calls it is the Advanced Cybersecurity Learning Platform (ACLP). SANS has all levels of cyber security training from non-existent to more advanced practices already in place. The **Security Awareness Maturity Model: Figure 8**, created

by Lance Spitzner in a blog titled *Defining the Security Awareness Maturity Model*, shows the various stages of progression for a cyber security awareness program:

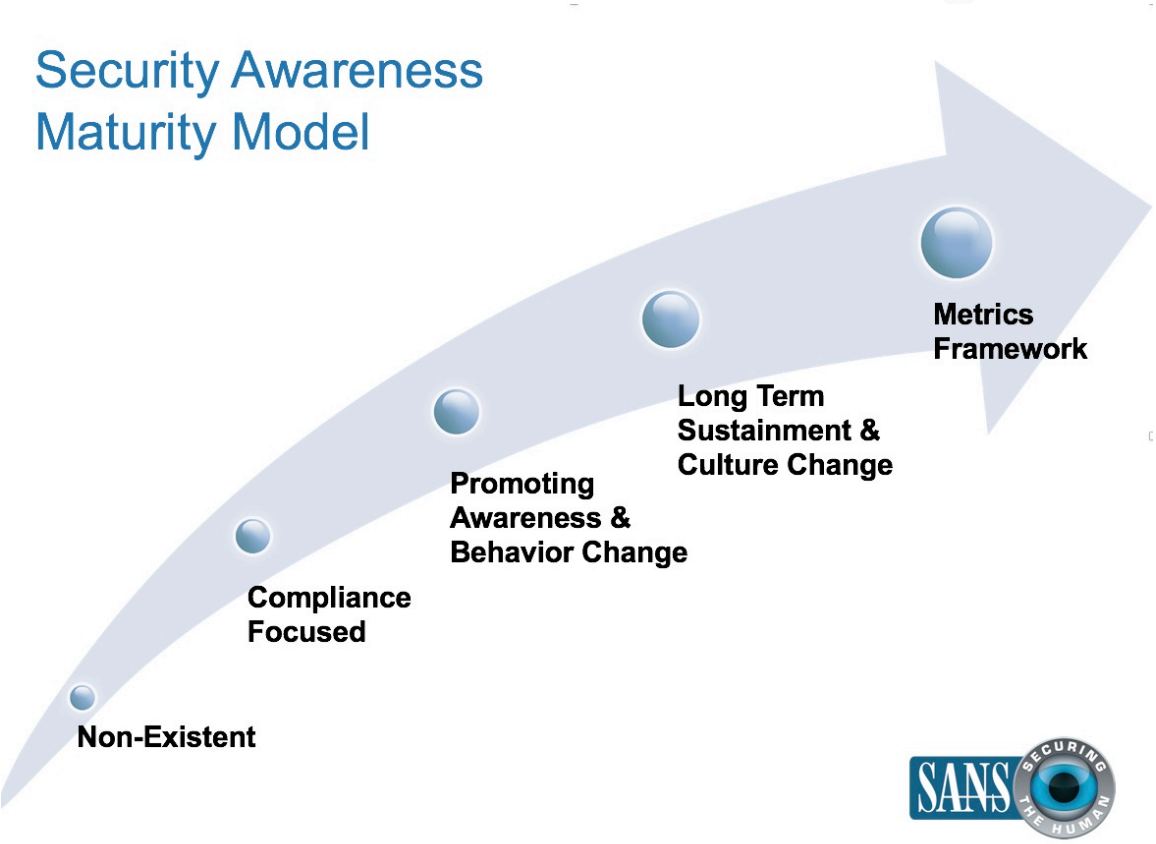

Figure 8: Security Awareness Maturity Model (Spitzner, 2016)

SANS offers a bootcamp course, *MGT433 Security the Human: How to Build, Maintain, and Measure a High-Impact Awareness Program*, in cyber security awareness training for security practitioners to teach them how to implement a program. The ACLP can be used in an organization to deliver training and scenarios to employees to educate them on threats in the industry. According to Lance Spitzer, SANS certified cyber security instructor with experience in cyber threat research, awareness and training, in his presentation *Making Awareness Stick* there are several different methods one can use to educate an employee base including the following:

- Computer-based Training (Training can be accomplished using the ACLP)
- Newsletters (SANS sends out a monthly OUCH! newsletter for security awareness)

Author Name, email@address

- Security Blog
- Promotional Items (Posters, notes, letters, etc.)
- Mascots/Taglines (Organization specific)
- Self-Education (Create a portal that employees can access with links to resources)
- Ambassador Program (Peer education)
- Gamification (Creating games that promote cyber security awareness)
- Salesforce (Security Champion Program that rewards good security practices)
- Leverage Leadership (Ensure leaders become educated promote to the workforce) (Spitzner, 2015)

As previously discussed, attackers often take advantage of human errors by crafting phishing emails tailored to entice a user to click a link or open a file. Attackers have been doing this for years and have become very good at manipulating users to perform a particular action that allows the attacker to gain control over the victim machine. An educated user, though, will go a long way into recognizing these threats and reporting them to security teams for examination. Although attackers have become experts at crafting seemingly believable phishing emails, there are many telltale signs that an educated user would recognize, such as an attachment for a parcel tracking or invoice service with a company they have no knowledge of using. Perhaps, hovering over a URL in an email to see that the link is a hyperlink to what appears to be a malicious website. These are notable signs of a potential threat, but if a user fails to understand these vectors of attack, they will not hesitate in clicking a link, especially should they spoof the sending name or email address. Therefore, it is important to implement a well-rounded cyber awareness program such as SANS' Securing the Human via their ACLP.

5. Conclusion

Email and Web Browsers account for the majority of successful compromises in any size organization within any industry. Evidence from Verizon, Symantec, FireEye all conclude that these two entry vectors are preferred and often successfully leveraged by attackers to gain an initial foothold in organizations. These threats are not limited to APT but are also leveraged by cyber criminals to deploy all types of malware from backdoors

to credential theft malware and even malware that is designed to steal credit card data from point-of-sale systems. Because email and web browsers pose such a high threat, it is imperative that organizations take immediate steps to address the Critical Security Controls that cover Email and Web Browsers security.

In addition to the threat posed by Email and Web Browsers, attacks perpetrated against employees of organizations use crafted emails containing either a URL to a malicious website or some type of attachment that will use social engineering to incite the user to enable content or scripts. Thus, it is important for organizations to take immediate steps to "Secure the Human" as noted by SANS. Organizations should implement a full-scale cyber awareness program that will educate users using education materials, scenario- based training, and awareness campaigns to secure the human element.

Whether organizations choose to secure one area over the other, both security controls are essential to ensuring protection against cyber threats. These controls are part of a broader security posture and will help in creating a layered defense. A layered defense will create firewalls that an attacker must overcome to breach an organization, resulting in a more secure defense.

Author Name, email@address

References

Aaron, G. (2016, May 23). Unique Phishing Sites Detected October 2015 - March 2016 [Chart]. In R. Manning (Ed.), *Phishing Activity Trends Report*. Retrieved July 15, 2017, from http://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf

Center for Internet Security. (2016, August 31). *The CIS Critical Security Controls for Effective Cyber Defense* [PDF]. Center for Internet Security.

FireEye. (n.d.). Cloud Email Security Datasheet | FireEye. Retrieved July 15, 2017, from https://www.fireeye.com/products/ex-email-security-products/email-threat-prevention-cloud-datasheet-pf-email.html

Group Policy Administrative Templates. (n.d.). Block macros from running in Office files from the Internet. Retrieved July 15, 2017, from http://getadmx.com/?Category=Office2016&Policy=excel16.Office.Microsoft.Policies.Windows%3A%3AL_BlockMacroExecutionFromInternet

Group Policy Administrative Templates. (n.d.). Configure extension, app, and user script install sources. Retrieved July 15, 2017, from http://getadmx.com/?Category=Chrome&Policy=Google.Policies.Chrome%3A%3AExtensionInstallSources

Group Policy Administrative Templates. (n.d.). Disable VBA for Office applications. Retrieved July 15, 2017, from http://getadmx.com/?Category=Office2016&Policy=office16.Office.Microsoft.Policies.Windows%3A%3AL_DisableVBAforOfficeapplications#

Microsoft. (2015, September 23). No Add-ins loaded due to group policy settings for Office 2013 and Office 2016 programs. Retrieved July 15, 2017, from https://support.microsoft.com/en-us/help/2733070/no-add-ins-loaded-due-to-group-policy-settings-for-office-2013-and-off

Microsoft. (2016, November 17). Set up SPF in Office 365 to help prevent spoofing. Retrieved July 15, 2017, from https://technet.microsoft.com/en-us/library/dn789058(v=exchg.150).aspx

Microsoft. (2016, December 9). Use DMARC to validate email in Office 365. Retrieved July 15, 2017, from https://technet.microsoft.com/en-us/library/mt734386(v=exchg.150).aspx

Author

Microsoft. (2016, December 16). Group Policy Administrative Template files (ADMX, ADML) and Office Customization Tool (OCT) files for Office 2013. Retrieved July 15, 2017, from https://technet.microsoft.com/en-us/library/cc178992.aspx

Microsoft. (2017, April 5). Enable and disable add-ons using administrative templates and group policy (Internet Explorer 11 for IT Pros). Retrieved July 15, 2017, from https://docs.microsoft.com/en-us/internet-explorer/ie11-deploy-guide/enable-and-disable-add-ons-using-administrative-templates-and-group-policy

Microsoft. (2017, June 19). Use DKIM to validate outbound email sent from your custom domain in Office 365. Retrieved July 15, 2017, from https://technet.microsoft.com/en-us/library/mt695945(v=exchg.150).aspx

Oglesby, R. (2011, November 14). How to Disable Firefox Auto Updates. Retrieved July 15, 2017, from http://blog.unidesk.com/how-disable-firefox-auto-updates

Organization Intrusion Data [E-mail interview]. (2017, June 10)

Organization Intrusion Data [E-mail interview]. (2017, June 16)

Organization Intrusion Data [E-mail interview]. (2017, June 19)

SANS. (n.d.). Security Awareness Solutions. Retrieved July 15, 2017, from https://securingthehuman.sans.org/cyber-security-awareness-solutions

Schwarzkopf, M., & Sammons, M. (2013, April 17). FirefoxADM. Retrieved July 15, 2017, from https://sourceforge.net/projects/firefoxadm/?source=typ_redirect

Spitzner, L. (2015, October 15). *Making Awareness Stick [PowerPoint slides]*. Retrieved from https://securingthehuman.sans.org/media/resources/presentations/STH-Presentation-MakingAwarenessStickv2.pdf

Spitzner, L. (2016, March 8). Security Awareness Blog. Retrieved July 15, 2017, from https://securingthehuman.sans.org/blog/2016/03/08/defining-the-security-awareness-maturity-model

Verizon. (2017, February 13). *2017 Data Breach Digest*. In *2017 Data Breach Digest*. Retrieved July 15, 2017, from http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest-2017-perspective-is-reality_xg_en.pdf

Verizon. (2017, April 27). *2017 Data Breach Investigation Report*. In *2017 Data Breach Investigation Report*. Retrieved July 15, 2017, from

http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf

Wueest, C. (2017, May). *ISTR Financial Threat Review 2017*[Scholarly project]. In *ISTR Financial Threat Review 2017*. Retrieved July 15, 2017, from https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-financial-threats-review-2017-en.pdf

Author