From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 9, 2018
Subject: Health Insurance Company (HIC) Corporate Anti-Malware Policy

Anti-Malware Policy Overview

The HIC Anti-Malware policy is intended to secure HIC business operations from business disruption and safeguard information by maintaining access to authorized users. It is the responsibility of the Chief Information Security Officer (CISO) to establish the HIC Anti-Malware Policy, Information Security Awareness Program (ISAP), and all associated policies to ensure users are knowledgeable of policies and procedures in the HIC Security Program.

Malware Definition: A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim (NIST, 2013). Malware is an umbrella term that stands for a variety of malicious software, including Trojans, spyware, worms, adware, ransomware, and viruses (Zamora, 2018).

Strategy One, Defense in Depth: Aim is 100% coverage of devices with an anti-virus and/or anti-malware platform capable of running or being protected by the platform with significant activity logged and centralized on the same or different security platform. Defense in depth includes encryption of data at rest and in transit. Additionally, protecting devices and traffic facing the internet (e.g. router) and disabling vulnerable services such as SMB and changing default administration credentials (Talos, 2018). Finally, it includes a comprehensive backup plan to transmit data to external sites to render ransomware ineffective.

Strategy Two, Offensive Security: Security based on best practices may equate to outdated security depending on the source. The threat landscape is constantly evolving with researchers discovering attack vectors almost on a weekly basis for a variety of systems. Therefore, a threat intelligence process is required to effectively deter cyber attacks with strategic, operational, and tactical intel. This enables an integrated threat driven approach to cyber security.

Scope

The policy applies to all information systems and connected devices owned and operated by HIC or its subsidiaries. This policy explicitly includes any system for which HIC has a contractual obligation to administer. This includes all systems for internal use by HIC and its subsidiaries regardless of whether HIC retains administrative obligation or not (SANS, 2013).

I. Anti-Malware Policy

The Chief Information Security Officer (CISO) or their designee shall ensure:

- Procedures and tools MUST exist to guard against, detect, and report malicious software
- IT personnel WILL BE trained and proficient in the use of the security solutions used to protect against malicious software
- End users are aware of the security policies and ENFORCED on their workstations
  (CDE, n.d.)

A. Computing Assets

All devices, servers, routers, and other network devices collectively known as "endpoints" MUST have protections from malware and its effects. An anti-malware solution must be applied to any endpoint whether connected to the HIC network or acting as standalone units. The following procedures shall be followed:

- Virus protection software MUST NOT be disabled or bypassed, this includes:
  - Remote access configuration and protocols to initiate remote access and meetings with vendors
  - Administrative password changes without consent of the CISO or Antivirus/Malware administrator
  - Windows processes disabling virus protection
- Setting for the virus protection software MUST NOT be altered in a manner that will reduce the software effectiveness
- Automatic update frequency CANNOT be altered to reduce the frequency of updates. Update times include the following minimum times:
  - Servers: updated within 2 days of updates release by the administrator assigned by the CISO
  - Clients/Workstations: updated within 7 days of release by the administrator assigned by the CISO
- All servers attached to the HIC network MUST utilize HIC approved/standard virus protection software and setup to detect and clean viruses
- All electronic mail gateways, devices, and servers MUST use HIC approved e-mail virus/malware/spam protection software and must adhere to HIC rules for the setup and use of this software. Only exception includes isolation of network device through separate VLAN with no access to file shares.
- Any threat that is not automatically cleaned, quarantines, and subsequently deleted by malware protection software constitutes a security incident and MUST be reported to the designated IT or security team. A user is REQUIRED to:
  - Inform the HIC Help Desk and/or Security Team immediately.
  - Switch off the machine (at the wall socket) and ensure no one else uses it
  - Gather any media that was used for transporting information in and out of the machine to be made available to the security team
  - Submit a security report
  - NOT use the PC (or suspected media) until it has been cleared as being safe to use.
    (Southern Health, 2016)
- Antivirus/Antimalware signature updates shall occur on a frequency defined by the CISO but shall occur minimally once each calendar day
  (CDE, n.d.)

B. Patch Management

In 2017, the time between patch and worldwide outbreak is as short as two months. This was the case for the WannaCry outbreak that took advantage of Microsoft's SMB Vulnerability (Fruhlinger, 2017). HIC's CISO MUST maintain the documentation for all hardware and software specifying the patch management process.

Servers: No more than 45 days behind available and tested security patches
Desktops and Laptops: No more than 62 days behind available and tested security patches. Application program should cover over 90% of systems on or connected to the network
Networks/Other: No more than 45 days behind available and tested security patches for routers and appliances managing LAN and internet traffic.

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 9, 2018
Subject: Health Insurance Company (HIC) Corporate Anti-Malware Policy

C. Application Installation and Management

Restricted Download Rights: Following the principle of "least privilege" no programs or executable files MUST NOT be downloaded from the internet and installed on devices without permission from the HIC Security Team.
Application Whitelisting: A list of applications approved for business and department MUST be created and maintained by the HIC Security Team. These applications will be added to the exception list in the antivirus application following configuration policies.
Script Control: CMD prompt in the Windows OS MUST be disabled for client devices to avoid commands that download programs or updates. Known malicious scripts or program code (e.g. Python) may be added to the antivirus application.
Testing: HIC security team MUST pentest that antivirus and antimalware will enforce application, script, and exception controls.

D. Administrative/Privileged Access Rights

Administrative groups will be created according to department or business need to be in accordance with the principle of "best fit access privileges". This is set up to ensure users have minimum level of privileges and reduce administrative tasks by applying rights individually. (Southern Health, 2016).

Default Credentials: Default administrative credentials provided by the software, manufacturer, or IT team provided by physical or electronic document to its user MUST be changed upon installation or use of the software or hardware. HIC users shall refer to the HIC password policy.
Exception: In the case a user will need admin rights, the user MUST be trained from technical staff about the use of an administrator profile on their device. Additionally, in the case of many users obtain admin rights (e.g. management or senior staff) a privilege management platform should be installed to log activity on admin profiles.

E. Boundary Protection/Firewalls

HIC local networks are to be protected by Firewalls on the boundary to the internet. Web proxy and filtering MUST be used to control exposure to internal IP addresses, access to websites, and scans connected sessions for malware (Southern Health, 2016).

F. Mail Server Anti-Virus

Mail & Attachments: Solution MUST automatically check for virus/malware before it enters or leaves email system (Southern Health, 2016). Mail server MUST have either an external or internal anti-virus scanning applications that scans all mail destined to and from the mail server (SANS, 2013).
DLP & Email Encryption: Solution MUST support capability for data loss prevention (DLP) and email encryption to protect customer PII and ePHI (Gartner, 2017)
Maintenance: Local anti-virus scanning applications MAY be disabled during backups if an external anti-virus application still scans inbound emails while the backup is performed (SANS, 2013).

G. SQL Server Anti-Virus

Real-time scanning MUST be turned off and scheduled scans must run during off hours to avoid performance degradation. Due to the size of memory allotted to SQL databases, a real time scanner will re-scan each change to memory possibly throwing out data and making the server run slower over time (Taylor, 2014).

- All inbound traffic should be sent through a centralized scan on a hardware device (e.g. firewall) before being allowed into the network.
- Secure the network by preventing LAN users from installing applications or accessing anything outside of the scope of their business duties.
- Content filters to be places to prevent access to websites that do not pertain to business duties.
- Email scanning solution to scan attachments prior to downloading.
  (Taylor, 2014)

H. Supporting Controls

Not one defense mechanism is effective without its supporting defenses known as "layered defense". The following are expected to coincide with the Anti-malware policy:

- Installation of server and workstation operating systems follow vendor best practices and recommended hardening after deployment.
- Hardening of the MS Active Directory for SQL has been performed and logging is enabled.
- The recommended best practice of network segmentation is used to reduce HIPAA systems and network scope.
- Required logging support systems and ideally SIEM functionality are deployed and pervasive.
- Alignment of technical controls with actual healthcare Covered Entity and Business Associate missions, roles, responsibilities, policies, procedures, baselines, mandates, etc.
- Physical and organizational controls and established and enforced.
- Presence and/or availability of IT staff at HIC and IT and Business Associates.
- Sufficient database backups are created regularly and transmitted securely offsite
  (Krueger, 2017)

I. Policy Compliance & Management

The HIC Security Team is tasked to verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner (SANS, 2013).

Exceptions: Any exception to the policy must be approved by the HIC Security team in advance (SANS, 2013). Major changes to this policy is not without approval of the CISO.
Non-Compliance: An employee found to have violated this policy MAY be subject to disciplinary action, up to and including termination of employment (SANS, 2013).
Audit Controls and Logs: HIC IT teams shall maintain antimalware installation and update logs, scan history logs, procedures for quarantine and removal, and document remediation and communication procedures for large scale incidents.
Distribution: This policy is to be distributed to all HIC staff and users of HIC information systems using hardcopies upon hiring or contract creation and available on the HIC intranet site.

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 9, 2018
Subject: Health Insurance Company (HIC) Corporate Anti-Malware Policy

Supplemental I: Definitions

TERM	DEFINITION
Anti-Virus (AV)	Software provides an electronic defense mechanism mitigating the risk of a computing device being infected with or affected by malware.
Virus	A computer virus is a computer program that can copy itself without permission or knowledge of the user. A virus can only spread from one computer to another when its host is taken to the uninfected computer; for instance, by a user sending it over a network or carrying it on a removable media.
Worm	A computer worm is a self-replicating computer program. It uses a network to send copies of itself to other PCs on the network and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms always harm the network (if only by consuming bandwidth), whereas viruses always infect or corrupt files on a targeted computer.
End Points	All devices (from servers to clients to networked equipment) with an operating system that is capable of being affected or infected by malware.
Malicious Software	Software designed to infiltrate or damage a computer system without the owner's informed consent.
Malware	A term derived from the words "malicious" and "software". The expression is a general term used to refer to a variety of forms of hostile, intrusive, or annoying software or program code.
Social Engineering	A technique used by attackers to attempt to subvert security controls, by attempting to convince a legitimate user to divulge sensitive information such as passwords, IP Addresses or details of security mechanisms in use or to enable others to do likewise, or to run inappropriate malware.
Spyware	A type of malware designed to collect information from the target system and transmit that data to external parties for unauthorized use. Most commonly packaged with legitimate (or seemingly legitimate) software, spyware installs itself without the user's knowledge
Spam	Unsolicited email, is email received from an unrequested source, which attempts to convince the user to perform an action (usually to purchase goods or services or click on a link).
Trojan Horse	A program that contains or installs a malicious program (the 'Trojan'). The term is derived from the classical myth of the Trojan horse. Trojan horses may appear to be useful or interesting programs (or at the very least harmless) to an unsuspecting user but are actually harmful when executed.
Rootkits	A stealthy type of software, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer.
Adware	A software package which automatically renders advertisements.
(Southern Health, 2016)	

What's the difference between antivirus and anti-malware?
Antivirus usually deals with the older, more established threats, such as Trojans, viruses, and worms. Anti-malware, by contrast, typically focuses on newer stuff, such as polymorphic malware and malware delivered by zero-day exploits. Antivirus protects users from lingering, predictable-yet-still-dangerous malware. Anti-malware protects users from the latest, currently in the wild, and even more dangerous threats. In addition, anti-malware typically updates its rules faster than antivirus, meaning that it's the best protection against new malware you might encounter while surfing the net. By contrast, antivirus is best at crushing malware you might contract from a traditional source, like a USB or an email attachment (Zamora, 2018).

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 9, 2018
Subject: Health Insurance Company (HIC) Corporate Anti-Malware Policy

Supplemental II: Summarized Practices

POLICY	PRACTICE DESCRIPTION
Attachments	Never open an e-mail attachment from a source that is not trusted or known.
Encryption	Always encrypt sensitive data that leaves the confines of a secure server; this includes encrypting laptops, backup tapes, e-mails, etc.
Layered Defense	Use an approach that establishes overlapping layers of security as the best way to mitigate threats.
Lease Privilege	The principle of least privilege is that individuals should have only the access necessary to perform their responsibilities.
Best Fit Privilege	The principle of best fit access privilege holds that individuals should have the limited access necessary to fulfill their responsibilities and have their access managed efficiently.
Patch Management	Be sure all network devices have the latest security patches including user desktop and laptop computers. Patch management is an essential part of a layered defense. Even when you do everything right, there may be a vulnerability in the vendor's system or application. An effective patch management program mitigates many of these risks.
Unique Identity	All users accessing information must use unique credentials that identify who they are; the only exception is public access of a public facing Web site.
Virus Protection	Virus and malware prevention must be installed on every device connected or stand-alone that is managed by the organization.
(Johnson, 2015)	

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 9, 2018
Subject: Health Insurance Company (HIC) Corporate Anti-Malware Policy

Supplemental III: Network Challenges

PRIMARY OBJECTIVE: REDUCE IMPACT OF RANSOMEWARE		
Threat	**Challenge**	**CONTROLS**
Ransomware	Clicking on phishing campaigns	1. Mail protection platform 2. MS Exchange Configuration 3. Security Awareness Program
	Multiple mapping to file shares	1. Real-time scanning of endpoint devices 2. Access controls to file shares
	Endpoint user files are encrypted	1. Decoy VLAN and files 2. Real-time alerts of malicious activity
	Backups and recovery services equated to 2-3 days loss attempting to bring environment back to 100%	1. Backup process and file integrity are tested 2. Backup and Continuity Plan created and analyzed
"Challenge" column by (Giuliano & Spaulding, 2017)		

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 9, 2018
Subject: Health Insurance Company (HIC) Corporate Anti-Malware Policy

Supplemental IV: Sophos Recommended Anti-Virus Setting

FEATURE	DESCRIPTION	SETTING
SCANNING		
On-access scanning	On-access scanning of archived files consumes a lot of memory. If on-access scanning of archived files is in use, every time such a file is viewed in Windows Explorer the contents of that file will be fully checked. If the file is a self-extracting archive, the self-extractor component will be checked with the default on-access scanning settings. So, checking the whole file, every time, with on-access scanning is unnecessary. The increased memory and CPU usage caused by scanning archived files is wasted if the file is not then accessed. You should not need to use on-access scanning of archives on a workstation. 1) If you need to check an archive before opening it, use a right-click scan. The contents of the file will be checked by on-access scanning anyway, before you run them. 2) If you need to check a group of archived files, place them all in the same folder and right-click scan that folder. 3) If you need to check archived files on a file server, use a scheduled scan. On-access scanning of archived files could be useful where a server is checking files before forwarding them to client workstations, e.g. as part of through traffic. It should not be part of a standard network setup	**Enabled**
Check files on - read	This should be switched on in practically all circumstances. On-access scanning provides virus checking for your workstations. All files that are opened by the computer are checked before they are run.	**Enabled**
Check files on – Rename	On-rename scanning can be useful in similar circumstances to on-write scanning, except that the file involved will have been written as if it were a non-executable file, then renamed to make it executable. You should use on-rename scanning in the same circumstances as on-write scanning.	**Enabled**
Check files on -Write	On-write scanning is useful when tracking the source of infection on your network, or if infected files are being written from over the internet. Files written to your hard drive by your computer, or another computer, will be checked when they are created. This will prevent a virus from spreading infected files over all open shares on your network. On-write scanning is particularly useful in tracing a virus that is spreading across network shares, but you should also check the use of file sharing on your network, particularly the security of administrative shares.	**Enabled**
Scan for - Adware and PUAs	Potentially unwanted applications (PUAs) are programs whose use should be carefully managed. Some of them (e.g. network access tools or instant messaging clients) may be useful to certain workers. If such a program is already in use on your network, and it is then added by Sophos to the list of potentially unwanted applications, it will be blocked immediately. Use scheduled scans to manage PUAs in an office environment. You can then decide which applications to allow, and which ones to block, without disrupting activity on your network.	**Enabled**
Scan for - Suspicious files		**Disabled**
Allow access to drives with infected boot sectors		**Disabled**
Scan inside archive files		**Disabled**
Scan system memory		**Enabled**
EXTENSIONS		
Scan all files	An 'All files' scan should be used to check that all components of a virus have been removed after disinfection, but it is not necessary in general use.	**Disabled**
Scan only executable and other vulnerable files		**Enabled**
Scan files with no extension		**Enabled**
CLEANUP		
Automatically clean up items that contain a virus/spyware	In Endpoint 10 the setting 'Automatically clean up items that contain a virus/spyware' for on-access scanning is enabled by default. Having this option enabled means there is less administrative work in dealing with malware reported to the console. This option also means you will not see items alerted in the Dashboard and/ or against the client computer's name in the console as the item of malware has been successfully dealt with. The alert history and reporting will include all events of malware detection though. We strongly recommend that you leave the follow up action as 'Deny access only'.	**Disabled**
If cleanup is not possible		**Deny access only**
Suspicious files		**Deny access only**
WEB PROTECTION		
Block access to malicious websites		**On**
Download scanning		**As on-access scanning**
BEHAVIOR MONITORING		
Behavior Monitoring		**Enabled**

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 9, 2018
Subject: Health Insurance Company (HIC) Corporate Anti-Malware Policy

Detect malicious behavior	Malicious behavior has to be enabled for HIPs protection and is the parent option to suspicious behavior. Disabling malicious behavior switches HIPs off completely. We recommend you keep this option checked.	**Enabled**
Detect malicious traffic		**Enabled**
Detect suspicious behavior	Suspicious behavior detects items that behave like malware but can be authorized if you recognize the file/ program. By default, the option is enabled but the pass-through option of 'Alert only' means the files will not be blocked.	**Enabled**
Alert only, do not block suspicious behavior		**Enabled**
Detect buffer overflows	Buffer overflow attacks can be a risk. However, as with suspicious behavior, if you recognize the file/ process that is running, then you can authorize the item.	**Enabled**
Alert only, do not block		**Disabled**
LIVE PROTECTION		
Live protection	Sophos Live Protection improves detection of new malware without the risk of unwanted detections. This is achieved by doing an instant lookup against the very latest known malware. When new malware is identified, Sophos can send out updates within seconds. In order to get this high level of protection, you should retain the default setting of 'Enabled'.	**Enabled**
Automatically send sample files to Sophos		**Enabled**
(Sophos, 2017)		

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 9, 2018
Subject: Health Insurance Company (HIC) Corporate Anti-Malware Policy

Supplemental V: Anti-Malware Controls under HIPAA

HIPAA SECTION	REGULATION	DESCRIPTION
General Security Standards 164.306	§164.306(A)	Covered entities and business associates must do the following: (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part; and (4) Ensure compliance with this subpart by its workforce.
Administrative Safeguards 164.308	§164.308(a)(1)(ii)(B)	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a)
	§164.308(a)(1)(ii)(D)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
	§164.308(a)(5)(ii)(B)	Implement procedures for guarding against, detecting, and reporting malicious software.
	§164.308(a)(5)(ii)(C)	Implement procedures for monitoring log-in attempts and reporting discrepancies
	§164.308(a)(6)(ii)	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.
Technical Safeguards 164.312	§164.312(b)	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information (ePHI).
Rule Controls, Breach Notification 164.404	§164.404(b)	(1) A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach. (2) Breaches treated as discovered. For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency)
(Krueger, 2017)		

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 9, 2018
Subject: Health Insurance Company (HIC) Corporate Anti-Malware Policy

Supplemental VI: AV Testing

ATTACK TEST PLATFORM	SCENARIO	VICTIM MACHINES

Kali Linux	**Social Engineering Attacks**
	• Vishing Attacks
	• Social Engineering Attacks
	  ○ Attachments:
	  ▪ Binary files
	  ▪ Macros
	  ▪ PDFs
	  ▪ Scripts
	  ○ Weblinks
	  ▪ Internet Explorer Exploits
	  ▪ Windows Exploits
	  ▪ Java Exploits
	  ▪ Gaining reserve shell & doing simple recon
	Browser Exploits
	Reserve Shell
	Endpoint Recon
	Windows Exploits
	Credential Dumping
	Lateral Movement
	Gaining Persistence
		Windows 10

(Giuliano & Spaulding, 2017)		

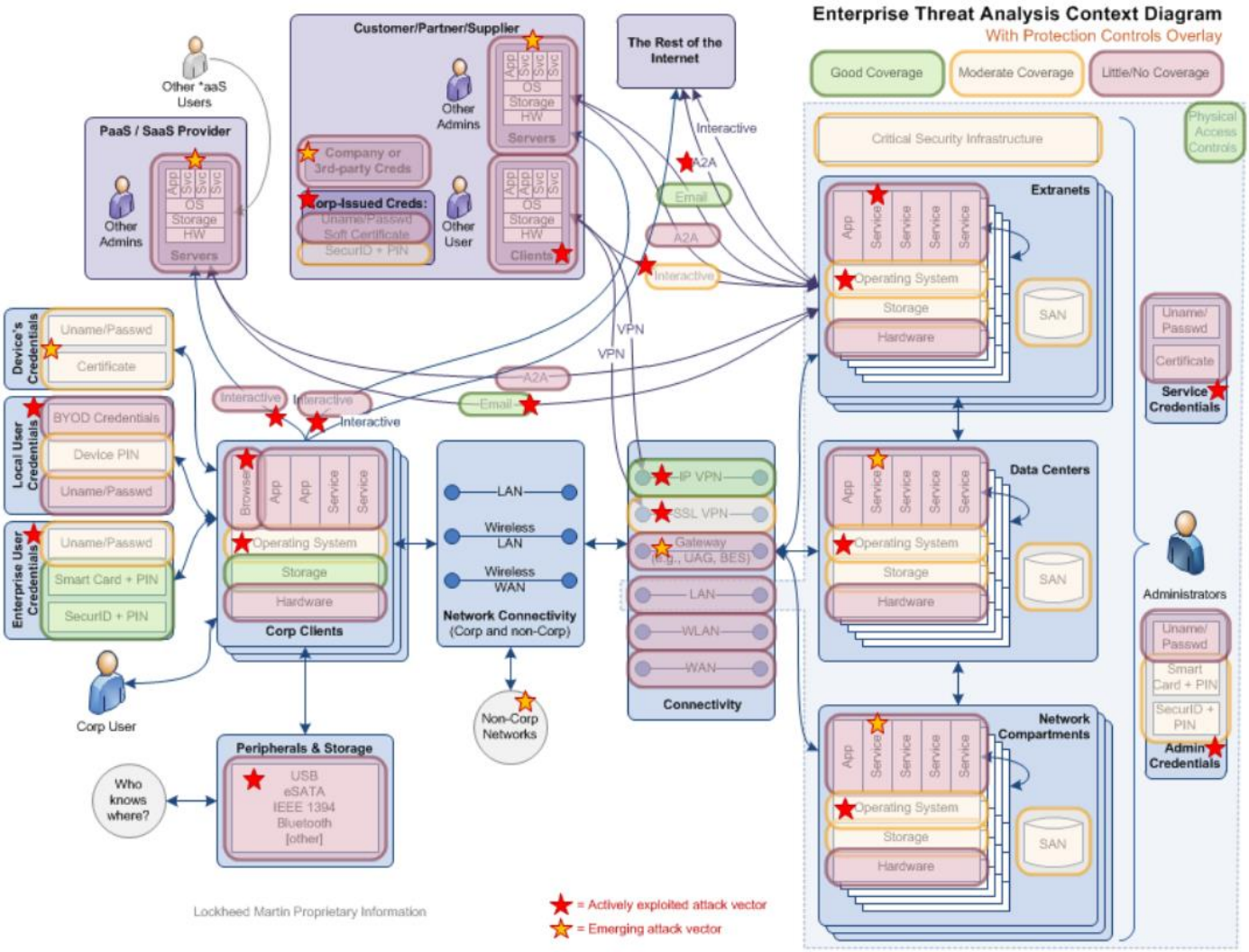
From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 9, 2018
Subject: Health Insurance Company (HIC) Corporate Anti-Malware Policy

Supplemental VII: User Types

USER CATEGORY	USER TYPE	DESCRIPTION
Human	Employees	*Salaried or hourly staff members of the organization.*
	Systems Administrators	*Employees who work in the IT department to provide technical support to the systems.*
	Security Personnel	*Individuals responsible for designing and implementing a security program within an organization.*
	Contractors	*Temporary workers who can be assigned to any role; contractors are directly managed by the company in the same manner as employees.*
	Vendors	*Outside companies, or individuals working for such companies, hired to provide ongoing services to the organization, such as building cleaning.*
	Guests & General Public	*A class or group of users who access a specific set of applications.*
	Control Partners	*Individuals who evaluate controls for design and effectiveness.*
Non-human	System Accounts	*Non-human accounts used by a system to support automated service.*
	Contingent IDs	*Non-human accounts until they are assigned to individuals who use them to recover a system in the event of a major outage.*
(Johnson, 2015)		

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 9, 2018
Subject: Health Insurance Company (HIC) Corporate Anti-Malware Policy

Supplemental VIII: Lockheed Martin's Enterprise Threat Analysis Context Diagram



(Lockheed Martin, n.d.)

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 9, 2018
Subject: Health Insurance Company (HIC) Corporate Anti-Malware Policy

Supplemental IX: HIC Help Desk or Security Team Checklist after Attack

TASK	CHECKBOX	NOTES
Check the infected PC		
Check any media that has been used with the infected PC.		
Check any other PC that the media has been used with		
Delete or clean any infected files		
Check any servers that may also have been accessed		
Try to determine where the virus may have originated		
Ensure the incident is completed within the appropriate timescales		
Ensure the user has completed a HIC incident report and forwarded to the risk management department, and inform the HIC's security team immediately		
Depending on the severity and impact of the incident a full incident report may be required and this will have completed by the HIC Security Specialist. Serious incidents are reportable to other authorities.		
(Southern Health, 2016)		

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 9, 2018
Subject: Health Insurance Company (HIC) Corporate Anti-Malware Policy

Supplemental X: HIC Policy Revision and Monitoring Compliance Tracking

MALWARE POLICY REVISISION HISTORY				
DATE OF CHANGE	**AUTHOR**	**VERSION**	**PAGE**	**SUMMARY OF CHANGE**
04.09.2018	R.NYE	1.0	All	New Policy
(Southern Health, 2016)				

MONITORING COMPLIANCE				
ELEMENT TO BE MONITORED	**LEAD AUTHOR**	**TOOL**	**FREQUENCY**	**REPORTING**
Policy Review	Name, Last Name	HIC Security Plan	1 year	HIC Security Team
AV Compliance	Name, Last Name	Antivirus Reporting Module	Weekly	As required by CISO, CIO
(Southern Health, 2016)				

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 9, 2018
Subject: Health Insurance Company (HIC) Corporate Anti-Malware Policy

Supplemental XI: Platform Technical Links

MS		
PLATFORM	**SUBJECT**	**MS Technical Link**
Server	*How to choose antivirus software to run on computers that are running SQL Server*	https://support.microsoft.com/en-us/help/309422/how-to-choose-antivirus-software-to-run-on-computers-that-are-running
	Analyzing System Performance	https://docs.microsoft.com/en-us/windows-hardware/test/wpt/whats-new-in-the-windows-performance-toolkit
MS Exchange 2016	*Antispam and antimalware protection in Exchange 2016*	https://technet.microsoft.com/en-us/library/jj150481(v=exchg.160).aspx
MS Azure Cloud Services	*Microsoft Antimalware for Azure Cloud Services and Virtual Machines*	https://docs.microsoft.com/en-us/azure/security/azure-security-antimalware
Citrix	*A Revolutionary Approach to Advanced Malware Protection*	https://www.citrix.com/blogs/2016/06/21/a-revolutionary-approach-to-advanced-malware-protection/
	Citrix Recommended Antivirus Exclusions	https://www.citrix.com/blogs/2016/12/02/citrix-recommended-antivirus-exclusions/
	Citrix Guidelines for Antivirus Software Configuration	https://support.citrix.com/article/CTX127030
Bitdefender	*Bitdefender Hypervisor Introspection (HVI)*	https://www.bitdefender.com/business/hypervisor-introspection.html
AWS	*Advanced Threats & Malware*	https://aws.amazon.com/mp/scenarios/security/malware/

From: Ryan Nye, CompanyX
To: Cameron Carter, HIC
Date: April 9, 2018
Subject: Health Insurance Company (HIC) Corporate Anti-Malware Policy

References

CDE. (n.d.). *Antivirus and Malware Policy.* cde.state.co.us. Retrieved from https://www.cde.state.co.us/dataprivacyandsecurity/antivirusandmalwarepolicy

Fruhlinger, J. (2017, September 27). *What is WannaCry ransomware, how does it infect, and who was responsible?* CSOonline.com. Retrieved from https://www.csoonline.com/article/3227906/ransomware/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

Gartner. (2017). *Securing Cloud-Based Email.* Gartner.com. Retrieved from https://www.gartner.com/imagesrv/media-products/pdf/Vade-Secure/Vade-Secure-1-4H8VR7F.pdf

Giuliano, L., Spaulding, M. (2017). *Lies, and Damn Lies: Getting Past the Hype of Endpoint Security Solutions.* Blackhat.com. Retrieved from https://www.blackhat.com/docs/us-17/thursday/us-17-Giuliano-Lies-And-Damn-Lies-Getting-Past-The-Hype-Of-Endpoint-Security-Solutions.pdf

Krueger, C. (2017, November). *MALWAREBYTES ENDPOINT SECURITY WITH HIPAA*. Malwarebytes.com. Retrieved from https://www.malwarebytes.com/pdf/white-papers/Coalfire_HIPAA.pdf

Mucking, M., Fitch, S. (n.d.). *A Threat-Driven Approach to Cyber Security.* Lockheed Martin.com. Retrieved April 9, 2018 from https://lockheedmartin.com/content/dam/lockheed/data/isgs/documents/Threat-Driven%20Approach%20whitepaper.pdf

NIST. (2013, May). *NISTIR 7298 Revision 2. Glossary of Key Information Security Terms.* Nist.gov. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

SANS Institute. (2013). *Server Malware Protection Policy.* Sans.org. Retrieved from https://www.sans.org/security-resources/policies/retired/pdf/server-malware-protection-policy

Sophos. (2017, November 16). *Recommended settings for Anti-Virus and HIPS.* Retrieved from https://community.sophos.com/kb/en-us/114345

Southern Health. (2016, September 12*). Anti-Virus and Anti-Malware Policy Version: 2*. southernhealth.nhs.uk. Retrieved from http://www.southernhealth.nhs.uk/_resources/assets/inline/full/0/73237.pdf

Talos. (2018, March 20). *EPISODE 25: WE'LL DO IT LIVE!!* [Audio Podcast]. Talosintelligence.com. Retrieved from https://www.talosintelligence.com/podcasts

Zamora, W. (2018, February 21). *What's the difference between antivirus and anti-malware?* [Web Blog]. Malwarebytes.com. Retrieved from https://blog.malwarebytes.com/101/2015/09/whats-the-difference-between-antivirus-and-anti-malware/

Logo from:

MarksMan Healthcare Communications. (n.d.). *HEOR – INDIA CONCLAVE (HIC).* Bna.com. Retrieved March 14, 2018 from https://marksmanhealthcare.com/heor-india-conclave/