Secure-IT Cyber Smart Assessment

Created by:
Matthew S. Almendinger

Published:
Oct. 1st, 2020

LIGHTHOUSE
IT SOLUTIONS

About My Network

Why don’t we kick things off with a little introduction?
Tell us about yourself:

My Company:

My Name:

My Role/Title:

Number of computers:

Number of servers:

Do you offer WIFI?

Technology

While technology is often the first thing we think of when we hear cybersecurity – in reality, however, it is usually the last defense to an attack. That, however, does not mean that you should neglect investing properly in it.

Let’s take a look at your technology stack to make sure that everything is tip-top shape.

Antivirus Protection

We’ll start off with the most common of technological weapons that we have: Antivirus. Antivirus should be installed on every computer that is on your network – and should be periodically checked to make sure that it is running properly and has not detected any threats.

Are you a Lighthouse Harmony Client? Check here and skip ahead!
We use policy detection to ensure that all domain-joined computers are installed with antivirus and enforced by our Insight Agent. Inconsistencies in the antivirus are reported to our Ticketing system for resolution. Our antivirus solutions, Sophos, utilizes Intercept-X for signature-less detection of threats that may be new and have not yet been detected before (called “zero-day” threats).

Are you using an antivirus product? Which one?

Has it been ensured that antivirus has been installed on all network-connected computers?

Has each computer been reviewed for status of the antivirus and that any detected threats have been cleaned or removed?

Does your antivirus use signature-less detection (often called “Nextgen Antivirus”)?

Do you use lockdown or application whitelisting to prevent unknown applications from running?

Managed Threat Detection and/or Response

Managed Threat Detection (MTD) and Managed Threat Response (MTR) are newer solutions that have been entering the marketplace. The purpose of MTD and MTR are very similar, but with a larger difference. With Managed Threat Detection, a utility performs "surveys" of your client systems to detect potential remnants of previous attacks. These remnants that are often left behind from successful clean-up by your antivirus is a mixed bag of good and bad. On the good, it means that the attack was thwarted by your antivirus software, however, it also means that a potential foothold for your computer was left behind. With enough knowledge or brute force, this remnant (or foothold), may be reutilized by a secondary attack without additional detection by your antivirus.

A good MTD solution provides notification of possible detection and feedback on how to remove the foothold.

Managed Threat Response is very similar to Managed Threat Detection, however, upon detection of a threat, the service will additionally provide remediation response and access to a Security Operations Center.

Are you a Lighthouse Harmony Client? Check here and skip ahead!
Your Harmony subscription includes access to the Huntress Managed Threat Detection platform and provides surveys of every client computer every 15 minutes. If an abnormality is discovered, it is submitted to a research team at Huntress for review. A remediation plan is built and returned to us at Lighthouse to execute. The Huntress platform also utilizes Ransomware Canaries to detect ransomware attempts in progress and help lock the system down.

Does your organization use an MTD or MTR solution? If so, which one?

Do you review the status of your clients in the solution regularly to ensure that it has been deployed to all active devices?

Local Administrative Access Control

Allowing users to have local administrative access can make overall support much easier, however, it also allows the risk of unwanted applications to be run with disastrous results.
Limiting administrative access protects your users from executing malicious software – thereby protecting your network.

(Note from Lighthouse IT: In the past, this has created some headaches for organizations that use outsourced IT providers, however at Lighthouse we have a hybrid solution that allows whitelisted applications to be run as necessary with protected administrative access without giving the user full access to the machine. Any programs not on the whitelist are sent to our helpdesk for review and approval, this allows us to provide the best of both worlds!).

Are you a Lighthouse Harmony Client? Check here and skip ahead!
Our Administrative Whitelisting product is coming very soon to your client computers and will be distributed via our Insight Agent when it is ready for your account.

Do you allow users to have local administrative access to their computers? If so, what is the percentage of users that have local administrative access?

Patch Management

One of the easiest ways to protect your network is to ensure that you are using up-to-date software. Routine patching can keep vulnerabilities minimized and lower the chance of compromise.

With all good things, however, make sure that you're checking in on your systems and that they are successfully installing those patches!

Are you a Lighthouse Harmony Client? Check here and skip ahead!
Our Insight agent features automated patch management for Windows as well as many widely popular applications.

Are your systems set to install operating system updates automatically?

Do you routinely check and install third party application updates, as well?
If so, how often?

Edge Security & Content Filtering

Secure networks must go beyond themselves. Protecting the edge of your network as it communicates with the internet is very quickly becoming the focus of organizations as they build proper defenses. Implementing a solution that can prevent access to potential threats can keep your network safe before it even enters. Additionally, utilizing content filtering can not only prevent access to shady websites but can also improve productivity as well.

Most edge protection features are provided by next generation firewalls.

Does your firewall support Network Edge protection features such as IP threat detection, Malicious Software scanning, application scanning, and/or content filtering?

Do you utilize any of these features? If so, which ones?

Do you use content filtering?

Multifactor Authentication

Password compromise is one of the most widely used methods of infiltration by cyber-attackers. Well-crafted phishing attempts can fool users into handing over their credentials without hesitation, giving authorized access to unauthorized persons.

Multifactor authentication combats this by creating a "zero-trust" layer with credentials. By adding a secondary authentication measure that utilizes a trusted device, such as a smart phone or hardware authenticator can prevent unauthorized users from gaining access even when they have the correct credentials.

Do you utilize MFA or 2FA for critical systems or systems that are publicly facing?

Which applications do you require MFA for?

Are there any critical applications that you do not use MFA for? Does the vendor support MFA?

Network Auditing

Even with best effort, vulnerabilities can exist. Auditing your network via regular scans or even utilizing an ethical hacking service can ensure that any open vulnerabilities that you do have can be safely rectified.

Do you perform regular vulnerability and port scans of internal and external resources? If so, how often?

Do you perform regular ethical hacking or penetration tests by a third party? If so, how often?

Password Management

Password Managers are very quickly becoming common tools to help with password compromise. Password Managers work by allowing you to generate complex passwords for each site that you use and filling them in when you need to log in.

By using a password manager – no two sites use the same password, reducing the chance that a password compromise can do any serious damage. The auto-fill feature also bypasses keyloggers – making it harder for an infected computer to exploit your passwords.

Do you use a password manager? If so, which one?

Device Encryption

Passwords may keep the computer's live system secure from unauthorized access – but that doesn't protect the data on the disks. If physical access to the hardware can be gained, data could be transferred from the computer – or even malicious payloads deployed to the device.

Device Encryption creates a trust between the hardware that it is running on and the drive – making the data unreadable outside of that hardware set.
Using Device Encryption keeps the local data safe – which is especially useful for the mobile workforce when equipment could easily be stolen or lost.

Do you use Device Encryption? If so, is the policy for mobile devices or all devices?

Do you backup the recovery keys in case data recovery is ever necessary?

Role-based Permissions

With role-based permissions, members or staff (or other system users) are assigned particular roles. Through those role assignments acquire the permissions needed to perform specific system functions. These permissions allow users to perform certain operations. For example, say you only want a specific level of employee to access a system or password.

Does your company enforce some sort of permissions system for their employees?

Do employees have access to only their job-specific information?

Do employees have permissions based on their job at the company?

Remote Access

Let's face it, working from home as gone from a company perk to a business necessity this year. Protecting your staff becomes hard when they could be working from anywhere – but it has become our largest priority.

Making sure that appropriate security protocols are in place means allowing employees to use personal devices for remote access a very big red flag. A company-managed device may cost you a couple hundred dollars now – but it could be the thing that saves you millions later.

Do you allow employees to remotely connect using personally owned devices to your network? If so, are there system health requirements for those devices?

Are any internal systems (such as a company intranet or business management system) public facing?

Do you require and use VPN or Software-Defined Perimeter?

Do public resources (such as public facing systems or VPNs) require MFA to access?

Preparedness

Being properly prepared allows your organization to respond swiftly and appropriately to potential compromise by implementing policies that protect your organizations and enforce a strong security culture. It also means establishing procedures to provide consistent and appropriate response to issues as they arise.

Physical Network Protection

Attackers are not just on the internet – they may be closer than you think. Protecting your infrastructure means protecting it physically as well. Make sure that important equipment is locked, and access is controlled. Likewise, it is recommended to disconnect or disable unused network outlets at the patch panel when they are not in use – especially if they are in common areas. You may also consider implementing port-based network access control to restrict what devices may communicate on your network.

Do you maintain access controls to your critical network infrastructure, such as servers, switches, firewalls, etcetera?

Do you disable unused network outlets or use 802.1X (Port-based Network Access Control)?

Wireless Network Protection

Wireless provides easy access to a network to any location within reach – but it can also be a stealthy point of entry to anyone that can pick up the signal. Properly securing your wireless protects your office from hidden visitors that could be sitting even in your parking lot!

Consider using WPA2-Enterprise to enable user-based authentication to your wireless network to prevent disgruntled ex-employees from wreaking havoc on your network. You'll also want to make sure that you are keeping firmware up to date to prevent exploit of your access points.

Do you use user-based authentication to authorize access to your company's wireless?

Do you frequently check for firmware updates for your access points and install?

Do you often cycle the pre-shared keys for networks that use WPA2-PSK (useful for legacy or consumer devices that need to access your network)?

Do you often review the client connection logs to verify that clients are expected and authorized?

Do you offer guest wireless? If so, is the wireless separate and isolated from your company network?

Has your guest network been verified that it cannot access local resources?

Bring-Your-Own Device (BYOD) Policing

Bringing a smartphone, tablet, or other mobile device may seem innocuous at first, however, allowing these devices on your network introduce an unmanaged device into a managed safe space.

Be sure to communicate acceptable use of employee-owned devices to your team and employ protections like public users, if offering WiFi (isolated, protected network).

Do you allow employee-owned devices to connect to the network?

If so, do you have an acceptable use policy defined and acknowledged by each employee?

Do you permit access to the internal network to employee-owned devices?

Do you require any security software or control on employee-owned devices?

Policies & Procedures

They may sound boring, but well-defined policies and procedures can protect your network by offering you a well-thought response when you need it most. In the heat of the moment, Incident Response Plans can rapidly organize teams and prepare your team, your company, and potentially your customers for how you will handle situation in the most level-headed manner.

Do you have a current Technology & Data Use policy to govern expectations with staff regarding safety protocols? If so, how often do you review it for appropriateness?

Do you have a current Incident Response Plan defining steps to take and who is responsible if a breach or incident were to occur? If so, how often do you review it for appropriateness?

Do you periodically assess your organization's cybersecurity health?

Do you follow or subscribe to resources that provide you with information regarding the latest breaches, threats, and cybersecurity news?

Contingency & Business Continuity

Falling hand-in-hand with being prepared is about having a contingency plan in place in case the worst happens. After verifying that the threat has been contained and removed, it is time to get back to business ASAP. A strong and well-documented disaster recovery plan coupled with reliable software allows for fast recovery in the case of any disaster.

In case of complete catastrophe – you may find that it is necessary to pay any ransom on your data and get additional help. Cybersecurity Insurance policies are no longer an optional idea – they are strongly recommended! A comprehensive Cybersecurity Insurance policy will help you every step of the way and protect your organization financially. A great policy also includes legal assistance and network analysis.

Are you a Lighthouse Harmony Client? Check here and skip ahead!
As a Harmony client, we require a BCDR solution that exceeds best practices. Our solution performs regular backups during the day, that is then replicated daily to our off-site partner. The end of each day, your server backups are tested using automation and virtualization. Once a backup is tested, a screenshot is performed – in the case of issue a ticket is created for review by a technician.

Does your backup solution capture system state of the devices it protects?

Do you perform backups at least daily?

Do you maintain an off-site backup? If so, where are the off-site backups stored?

Do you test your backups for completeness regularly? If so, how often?

Do you have a cybersecurity insurance policy? If so, how much (many policies are after thoughts and won't even protect against a fraction of the ransom, let alone recovery and legal fees)?

Habits & Training

Welcome to the real key to protecting your business. The reality is that your most vulnerable point of failure for security is also your strongest: Your team.

By empowering your team with education and proper security habits – you can stop cyberattacks in their tracks. A well-educated team can identify potential threats and respond and report possible failures faster than some attacks even take to get started.

Cybersecurity experts claim that increased training has drastically reduced the number of disruptive cybersecurity incidents and that nearly 90% of all cybersecurity incidents involve a phishing element.

Do you provide regular training to employees on proper security etiquettes and protocols?

Do you simulate attacks to identify employees that do not maintain adequate security posture?

Do you engage with employees regularly to discuss expectations and share news of common threats by cyber-attackers?

Is security training provided to all new hires?

Do you reward employees for exhibiting a strong posture and contributing to the safe culture?

Ready for review?

Head on over to to submit it to us:
https://content.lighthousesol.com/cybersmartupload

Once submitted, an expert at Lighthouse IT will be able to review the assessment with you and explain what state your network is in! You and your team can sit down together with a Lighthouse IT expert and plan out remedies to issues, or simply celebrate your spotless network!

On top of all that, we will give your organization access to 4 FREE cybersecurity tools!

This assessment was created by:
Lighthouse IT Solutions
info@lighthousesol.com
349 1/2 Rice St, Elmore, OH 43416
419.740.0825

Version: 1.0