Menlo Security

CREATING A SECURE HEALTH NETWORK FOR SINGAPORE

Implement COI's 16 cybersecurity recommendations without impacting user productivity

WHITE PAPER

INTRODUCTION

A major data breach that exposed millions of patient records forced Singhealth, the largest health network in Singapore, to rethink how it protects users from web-based cybersecurity threats. To its credit, Singhealth worked with the government’s cybersecurity agency to investigate who committed the largest breach in the nation’s history and how they were able to circumvent the organization’s defenses. A Committee of Inquiry (COI) released a report in January 2019 that outlined 16 recommendations that Singhealth and other organizations can do to mitigate future attacks.

In this white paper, we provide an overview of COI recommendations and guidance to organizations on how they can implement these cybersecurity policy changes.

A Most Egregious Breach

It was the most egregious data breach in the history of Singapore. In June 2018, hackers stole the personal data of more than 1.5 million patients, including prescription data for the prime minister. More than merely an embarrassment, the breach served as a warning to many public and private organizations throughout the region and the world. If Singapore, one of the world’s most connected countries, as well as one of the world’s most cybersecure, could have a breach of this magnitude perpetrated against a national institution, it could essentially happen to any organization anywhere.

It All Started with a Phishing Attack

According to the Cybersecurity Agency (CSA) of Singapore, the hacker was extremely deliberate throughout the attack, initially gaining access to a front-end computer at Singapore General Hospital through a highly-targeted phishing email. An innocent-looking link automatically installed custom malware on the device, and the hacker laid low for several months, waiting for the optimal time to strike. Eventually, he started to distribute malware and steal credentials, including those that ultimately gave him access to the Electronic Medical Record (EMR) database. He avoided secondary targets that may have drawn attention to his presence and was able to erase all traces of his activities. The attacker also planted multiple footholds in the network—later used to attempt re-entry into the Singhealth system.

Attack Profile Card

ATTACK NAME

Credential Phishing

TARGETS

Public agencies, political organizations and enterprises (essentially anyone with valuable information)

ATTACKERS

- Nation-state sponsored groups
- Advanced Persistent Threats (APTs)
- Cyber criminals
- Hacktivists

METHODS

- Mimic an authentic-looking login website
- Hijack an existing login page

BOTTOM LINE

Credential phishing attacks are often the beginning of a much larger and more destructive attack. Phishing emails are simply the way a threat actor gains access to the network before stealing information, making a ransom demand or simply creating havoc.

These types of phishing attacks are so successful because they play on the weakest link in any organization's security posture: the user. Attackers know very well how to manipulate human nature and emotions to steal or infiltrate what they want. They use email messages that induce fear, a sense of urgency, curiosity, reward and validation, an emotionally charged response by their victims or simply something that is entertaining and a distraction to convince, cajole or concern even seasoned users into opening a phishing email. In fact, 12 percent of users will open a phishing email while 4 percent will always click a link in a phishing email.[1] Enterprise users are little more discerning, but not by much. According to threat intelligence from Menlo Labs, 1.3 percent of the URLs in received emails were clicked across our customer base over the past 30 days.

This high success rate is why phishing attacks like the Singhealth breach are on the rise in nearly every enterprise segment. According to the latest Verizon Data Breach Digest, 72 percent of enterprise data breaches originate from phishing attacks.[2]

[1] 2018 Data Breach Investigations Report (11th Edition), Verizon

[2] 2018 Data Breach Investigations Report (11th Edition), Verizon

Air-Gapping: An Inefficient Solution

To its credit, Singhealth worked with the government's cybersecurity agency to investigate who committed the act and how they were able to circumvent the organization's defenses. The COI was set up and a months-long investigation begun. Unfortunately, before the COI could issue it's report, a knee-jerk reaction to implement new network separation policies started gaining support. Years before, the government had begun mandating that all endpoints connected to government networks be disconnected to the internet—and the noise was being made to extend those policies to all health networks as well.

The problem is that air-gapping—as network separation is commonly known—fails to provide 100 percent protection from web-based threats and attacks due to advanced attack techniques (see sidebar). At the same time, the act of separating user devices from the internet proved to be a major inhibitor to user productivity and workflows. So while the breach exposed how vulnerable Singapore's healthcare systems really were to web-based attacks, simply cutting off internet access was a non-starter. Users need access to web-based tools and information for reporting and research among other work-related uses.

As a result, Singhealth needed a cybersecurity approach that would guarantee 100 percent protection from these web-based threats without impacting the user experience. Fortunately, the COI agreed.

Dissecting the Report and Guidance

The COI issued a report in January 2019 that outlined 16 recommendations that range from improving incident response processes to creating better anti-phishing education for users. Seven of the recommendations were labeled a priority. According to the committee's chairman, retired chief district judge Richard Magnus, the recommendations "are aimed at enhancing responses to similar incidents, better protecting Singhealth's database against similar attacks and reducing the risk of such cyberattacks on public sector IT systems with large databases of personal data."

On the following pages is a summary of the COI's recommendations that are related to ensuring key processes are in place when it comes to securing networks. Menlo advises companies to take a look at their existing policies to ensure that partners and key integrations have been correctly documented when it comes to third-party access to data location.

Hardened processes and a clear line of responsibility will ensure that everyone who has access to sensitive data has a clear understanding of what is expected of them.

COI RECOMMENDATION	MORE DETAILS
An enhanced security structure and readiness must be adopted by the Integrated Health Information Systems (IHiS) and public health institutions.	• Cyber security has to be seen as a risk management issue, and not just a technical issue where decisions are made at the appropriate management level. • IHiS, Singapore's central IT agency for the healthcare sector, has to take an approach where security is not dependent on just one line of defence. Gaps between policy and practice must be addressed.
Online security processes must be reviewed to assess their ability to defend and respond to advanced threats.	• Effectiveness of current processes must be reviewed to fill gaps used by the attacker.
Enhanced security checks must be performed, especially on critical information infrastructure (CII) systems.	• Vulnerability assessments, safety reviews and certification of vendor products must be done.
Privileged administrator accounts must be subject to tighter control and greater monitoring.	• An inventory of administrative accounts should be created to keep track of them. • All administrators must use two-factor authentication (2FA) when doing administrative tasks. • Passphrases, instead of passwords, could be used. Password policies must be implemented and enforced. • Server local administrator accounts must be centrally managed. • Privileged service accounts must be managed and controlled.
There should be partnerships between the industry and the government to achieve a higher level of collective security.	• Threat intelligence sharing should be enhanced. • Partnerships with internet service providers should be strengthened. • Apply behavioural analytics.

ADDITIONAL RECOMMENDATIONS	MORE DETAILS
IT security risk assessments and audit processes must be treated seriously and carried out regularly.	• IT security risk assessments must be conducted on CII and mission-critical systems annually and upon specified events. • Audit action items must be remediated. • One key recommendation is that SingHealth appoint its own cyber-security "risk man" rather than rely solely on its IT management vendor, Integrated Health Information Systems (IHiS), for such oversight.
Enhanced safeguards must be put in place to protect electronic medical records.	• A clear policy on measures to secure confidentiality, integrity and accountability of electronic medical records must be formulated. • Have real-time monitoring of databases with patient data. • End-user access to electronic health records should be made more secure. • Controls must be put in place to better protect against data theft.
A software upgrade policy with focus on security must be implemented to increase cyber resilience.	• A proper governance structure must be in place to make sure policy is being followed appropriately.
Incident response plans must more clearly state when and how a security incident is to be reported.	• It must clearly state that an attempt to compromise a system is a reportable security incident and include examples as well as indicators of an attack.
Competence of computer security incident response personnel must be significantly improved.	• A competent and qualified security incident response manager who understands and can execute the required roles and responsibilities must be appointed.
A post-breach independent forensic review of the network, all endpoints and the electronic medical records system should be considered.	• IHiS should consider working with experts to ensure no traces of the attacker are left behind.

COI recommendations that can be impacted by Menlo Security

The following are COI recommendations that can be put into place by deploying a web isolation solution from Menlo Security.

COI RECOMMENDATION	MORE DETAILS
Staff awareness on cyber security must be improved to better prevent, detect and respond to security incidents. • The level of cyber hygiene among users must improve. • A security awareness program should be implemented to reduce organizational risk. • IT staff must be equipped with sufficient knowledge to recognize the signs of a security incident.	A key part of Menlo's solution is to ensure phishing attacks are mitigated and users are educated on identifying the characteristics of a phishing website. Menlo Security Email Link isolation ensures all links that are clicked in an email are automatically isolated. Once isolated, Menlo is able to provide custom banner and empower control to admins on what websites should be warned upon and what websites should not allow the user to input any data.
Domain controllers must be better secured against attacks. • Operating system for domain controllers must be more regularly updated to protect them against the risk of cyber attack. • Limit log-in access and require 2FA for administrative access.	With Menlo in place and all browser traffic from a Domain Controller being sent to Menlo Security, organizations can ensure that no active content (good or bad) is executed locally. This ensures malware does not even have a chance to execute on the prized asset: Domain Controller.
Improve incident response processes for a more effective response to cyber attacks. • Response plans must be tested frequently to ensure effectiveness. • A balance must be struck between containment, remediation and eradication, and the need to monitor an attacker and preserve critical evidence. • Information needed to investigate an incident must be available. • An Advanced Security Operation Centre or Cyber Defence Centre should be established to improve the ability to detect and respond to intrusions.	Menlo reduces the number of false positives by stopping attacks before they reach the network perimeter when an alert would be generated. This allows incident response teams to focus on the events that need attention while eliminating alert fatigue.

(continues on following page)

COI RECOMMENDATION *(continued)*	MORE DETAILS
A robust patch management process must be implemented to address security vulnerabilities. • Formulate and implement a clear policy on patch management.	Patch management is a major resource requirement for companies. IT requires coordination across different department, various testing and there is always an outage. With Menlo, customers can de-prioritize providing patch for browser vulnerabilities as no active content is executed on the user's browser. Implying that even if there was an outdated browser, it would no longer be vulnerable as Menlo is providing Isolated content which is not active!
An internet access strategy that minimises exposure to external threats should be implemented. • Internet access strategy should be considered afresh • The healthcare sector should consider the benefits and drawbacks of internet surfing separation and internet isolation technology, and put in place mitigating controls to address the residual risks.	Menlo enables a web isolation cybersecurity approach. See below why this is better than web separation.

WHEN NETWORK ISOLATION ISN'T ENOUGH

Network isolation has grown in popularity—especially for government and military organizations that require 100 percent protection from web-based attacks. The thinking is that since there is no way for a user's work device to access the internet and web, there is no way for their organization or their network to be attacked, hacked or breached. While this approach is potentially very secure it does have some significant downsides. New techniques developed by increasingly-sophisticated threat actors can access endpoints—even when the device is not connected to the internet.

- **USB Drives**: Can be used to transfer data downloaded from the internet from a network-separated device to a network-connected device.
- **Electromagnetic Waves**: Cell phone-based malware can be used to poach data via electromagnetic waves from network-separated systems.
- **Acoustic Signaling**: Circumvents network separation over an acoustical mesh network to steal data.
- **Airhopper**: Uses FM frequency signals from a nearby mobile phone to infiltrate network-separated devices.
- **Bitwhisper**: Uses thermal manipulation to steal data using a covert signal.
- **GGMem**: Uses cellular frequencies produced by a standard internal bus to convert the network-separated device into a cellular transmitter antenna to steal information via GSM frequencies.
- **Powerhammer**: Leverages current fluctuations in power lines supplying electricity to network-separated computers.
- **Magneto**: A technique for passing data from network separated computers to smartphones using electric fields.
- **Fansmitter**: Uses the fans in network-separated computers to send acoustic data.

The old adage, "Where there's a will, there's a way" holds true.

A Better Approach: Web Isolation

Using browser isolation or remote browsing, organizations can ensure that all web-based user activity—including webmail—is executed in a secure, trusted environment in the cloud. Since no web pages are actually executed on a user's endpoint device, the user cannot inadvertently unleash malware on their device or any other devices it is connected to throughout the corporate network.

But not all web isolation solutions are created equal. Virtual Desktop Infrastructure (VDI) and other isolation techniques deliver a slow, glitchy browsing experience. So while users are protected, they really aren't accessing the real internet—just a watered-down facsimile that eliminates many useful functions like copy, paste and print.

Instead, a web isolation solution from Menlo acts as a virtual browser in a cloud environment that operates on behalf of the user. The user's web browsing experience looks and feels consistent—because the user really is accessing real web content—just in Menlo's remote browser in the cloud rather than on their device. This prevents malicious content from ever reaching endpoints where it can do real damage.

Comparisons of Network Isolation vs Menlo Isolation Approach

PHYSICAL INTERNET SEPARATION	MENLO SECURITY ISOLATION PLATFORM
• Malware can be downloaded through other means (see sidebar) • Users having to use two computers disrupts workflows • Limited access to internet saps productivity • Additional capex and opex costs for separate devices • Devices reserved for "internet use" still at risk	• Web content is fetched and executed in a cloud-based browser, preventing malware from accessing users' devices • Web content is rendered in HTML5, giving users a consistent browsing experience • No client or special browser to install • No pixelated pages or noticeable latency • Preserves web functions such as copy, paste and print

Time to Make a Decision

Singhealth has already signaled that it is going to implement all of the COI's 16 cybersecurity recommendations in its report, but a major decision still needs to be made about the thirteenth recommendation that suggests a new internet access strategy is needed: web separation or web isolation?

The choice is simple.

On one hand, the government can mandate that all healthcare workers access the public internet on separate devices from network-enabled computers—forcing them to procure and use multiple devices. As we mentioned before, this would be an expensive mandate and dramatically impact workflows and productivity. It would also fail to protect users from web-based threats since threat actors have developed several innovative techniques to get around web separation policies.

Web isolation, however, requires no additional devices. Nor does it interrupt user workflows or change the web browsing experience. All web content can be isolated in a remote browser in the cloud, shielding users from any malicious code or credential theft attempt.

Take action today! Learn how you can protect your organization from today's increasingly sophisticated cyberattacks. Contact Menlo Security today at menlosecurity.com or sales@menlosecurity.com.

Menlo Security

About Menlo Security

Menlo Security's cloud-based Next-Generation Isolation platform scales to provide comprehensive web, email and document protection across enterprises of any size, without requiring endpoint software or impacting the end user-experience. Menlo Security is trusted by major global businesses, governments and verticals, including Fortune 500 companies and financial services institutions, and backed by leading venture capital firms and banks.

2300 Geng Rd., Ste. 200
Palo Alto, CA 94303
Tel: 650 614 1705
info@menlosecurity.com

menlosecurity.com