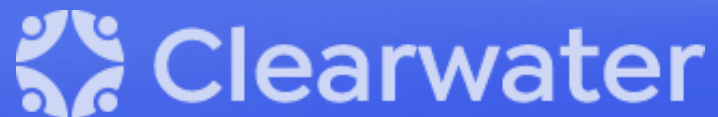


Monthly Cyber Briefing

July 11, 2024



Logistics

- All attendees in “Listen Only Mode”
- Please ask content related questions in Q&A
- Recording, final slides, and resources shared within 24 hours
- Please take a few minutes to provide feedback via survey prompt at the end of this session

Agenda & Speakers

- Cyber update
- How to engage your C-suite and board in effective and ongoing dialogue about Enterprise Cyber Risk Management



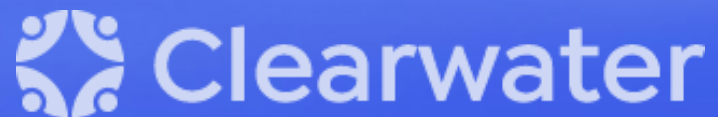
Steve Cagle
Chief Executive Officer
Clearwater



Bob Chaput
Founder & Executive Chair
Clearwater

Cyber Update

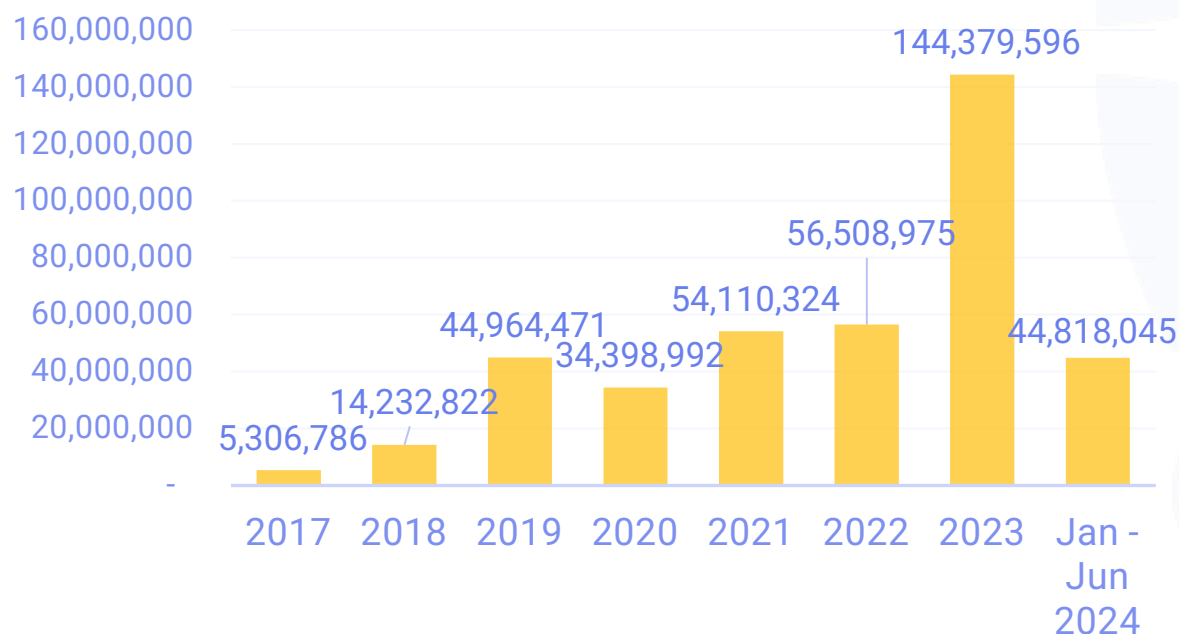
Steve Cagle



Breach Reports via OCR Breach Portal¹ and SEC

- 144.4M records reported breached in 2023, an increase of 156% vs 56.5 million in 2022
- 2024 – 44.8m records from 358 breaches reported, 12% decrease in the number of records breached first 6 months 2023, however increase of 7% in number of breaches reported

Healthcare Records Breached



Notable in June 2024 breach data

- Fewer breaches reported (42 vs. average 60/month for the first 6 months)
- Largest breach reported since last Cyber Briefing was A&A Services d/b/a Sav-Rx involving 2.8m individuals (ransomware)
- Geisinger experienced 1.2m record breach due to insider threat through business associate Nuance Communications, a division of Microsoft

Ransomware Attacks From “Newer” Threat Actors

Cyberattack led to harrowing lapses at Ascension hospitals, clinicians say

Attack commences on May 8th - Blackbasta

Urgent call for O-type blood donations following London hospitals ransomware attack

Attack commences on June 3rd - Qilin

Florida health department data captured in cyberattack, hackers claim

The Department of Health possesses some of the state's most sensitive data.

Attack commences on July 2 - RansomHub

RansomHub

RansomHub is growing into one of the fastest growing threat actors targeting healthcare.

```
README_9daasd.txt x
1 Hello!
2
3 Visit our Blog:
4   Tor Browser Links:
5     http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion/
6   Links for normal browser:
7     http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion.ly/
8
9
10 >>> Your data is stolen and encrypted.
11
12 If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your
13 data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for
14 a long time. The sooner you pay the ransom, the sooner your company will be safe.
15
16 >>> If you have an external or cloud backup; what happens if you don't agree with us?
17
18 All countries have their own PDPL (Personal Data Protection Law) regulations. In the event that you do not
19 agree with us, information pertaining to your companies and the data of your company's customers will be
20 published on the internet, and the respective country's personal data usage authority will be informed.
21 Moreover, confidential data related to your company will be shared with potential competitors through
    email and social media. You can be sure that you will incur damages far exceeding the amount we are
    requesting from you should you decide not to agree with us.
```

- Emerged February 2024 with over 45 victims so far
- Targeting Windows, Linux, and ESXi systems with malware written in Go and C++ and has attacked misconfigured Amazon S3 buckets
- Attracting former affiliates of BlackCat/APLHV and Lockbit, paying 90% commission rate
- For more information on detection and mitigation techniques access [Recorded Future's \(Insikt\) Threat research bulletin](#)



Qilin (aka Agenda)

Qilin is now the 4th largest ransomware threat actor, and actively targeting Healthcare.

```
-- Qilin
Your network/system was encrypted.
Encrypted files have new extension.
-- Compromising and sensitive data
We have downloaded compromising and sensitive data from you system/network
If you refuse to communicate with us and we do not come to an agreement, your data will be
published.
Data includes:
- Employees personal data, CVs, DL , SSN.
- Complete network map including credentials for local and remote services.
- Financial information including clients data, bills, budgets, annual reports, bank state
ments.
- Complete datagrams/schemas/drawings for manufacturing in solidworks format
- And more...
-- Warning
1) If you modify files - our decrypt software won't able to recover data
2) If you use third party software - you can damage/modify files (see item 1)
3) You need cipher key / our decrypt software to restore you files.
4) The police or authorities will not be able to help you get the cipher key. We encourage
you to consider your decisions.
-- Recovery
1) Download tor browser: https://www.torproject.org/download/
2) Go to domain
3) Enter credentials-- Credentials
Extension:
Domain:
login:
```

- Russian threat actor, began operations in 2022, formerly known as “Agenda”
- Recruiting affiliates since 2023
- 60 ransomware attacks since January 2024, including 15 on Healthcare and Public Health System, half of which were in U.S.
- Targets its victims through phishing and spear phishing emails and leverages exposed applications and interfaces such as Citrix and remote desktop protocol (RDP)
- Access the June 18, 2024 [HC3 Threat Profile](#) for more detail

Three HC3 Sector Alerts Since Last Briefing



Office of
Information Security
Securing One HHS

Health Sector Cybersecurity
Coordination Center

HC3: Sector Alert

June 04, 2024 TLP:CLEAR Report: 202406041700

Baxter Welch Allyn Vulnerabilities

Executive Summary

CISA recently published two ICS Medical Advisories for Baxter products, including Baxter Welch Allyn Configuration Tool and Baxter Welch Allyn Connex Spot Monitor (CSM). Both vulnerabilities received a CVSS v4 score of 9 or higher (CRITICAL), and are exploitable remotely. Successful exploitation of one of these vulnerabilities could result in an impact and/or delay to patient care. While a patch is currently available for one of these vulnerabilities, a software update will not be made available for the other until Q3 2024. Mitigations and workarounds from the vendor and CISA are outlined in this Sector Alert.

Report

On May 30, 2024, CISA published multiple ICS Medical Advisories for Baxter products and medical devices. The affected products include Baxter Welch Allyn Configuration Tool (versions 1.9.4.1 and prior) and Baxter Welch Allyn Connex Spot Monitor (CSM) (versions 1.5.2 and prior). Both vulnerabilities (detailed in the [Vulnerabilities](#) section) received a CVSS v4 score of 9 or higher and are exploitable remotely. Successful exploitation of these vulnerabilities could lead to the unintended exposure of credentials to unauthorized users and/or allow an attacker to modify device configuration and firmware data. Tampering with this data could lead to device compromise, resulting in impact and/or delay in patient care. According to Baxter: "Any credentials that were used for authentication or input while using the Welch Allyn Configuration Tool have the potential to be compromised and should be changed immediately." Despite this risk, Baxter stated that it has not found any evidence to suggest the flaw has been exploited in the wild, and plans to release a new software update to address the flaw in Q3 2024.

Analysis



These two vulnerabilities involve multiple common weaknesses. The first is "CWE-522: Insufficiently Protected Credentials" in which the product transmits or stores authentication credentials, but it uses an insecure method that is susceptible to unauthorized interception and/or retrieval. Automated static analysis, commonly referred to as Static Application Security Testing (SAST), can find some instances of this weakness by analyzing source code (or binary/compiled code) without having to execute it. Typically, this is done by building a model of data flow and control flow, then searching for potentially-vulnerable patterns that connect "sources" (origins of input) with "sinks" (destinations where the data interacts with external components, a lower layer such as the OS, etc.). The second is "CWE-1394: Use of Default Cryptographic Key" in which product uses a default cryptographic key for potentially critical functionality. It is common practice for products to be designed to use default keys. The rationale is to simplify the manufacturing process or the system administrator's task of installation and deployment into an enterprise. However, if admins do not change the defaults, it is easier for attackers to bypass authentication quickly across multiple organizations.

Vulnerabilities

- [CVE-2024-5176 \(CVSS v4 9.4\)](#): Insufficiently Protected Credentials ([CWE-522](#)) vulnerability in Baxter Welch Allyn Configuration Tool may allow Remote Services with Stolen Credentials. This issue affects Welch Allyn Configuration Tool: versions 1.9.4.1 and prior.
- [CVE-2024-1275 \(CVSS v4 9.1\)](#): Use of Default Cryptographic Key ([CWE-1394](#)) vulnerability in Baxter Welch Allyn Connex Spot Monitor may allow Configuration/Environment Manipulation. This issue affects Welch Allyn Connex Spot Monitor in all versions prior to 1.5.2.

[TLP:CLEAR, ID#202406041700, Page 1 of 3]

U.S. Department of Health and Human Services
Health Sector Cybersecurity Coordination Center (HC3) [www.HHS.GOV/HC3](#)



Office of
Information Security
Securing One HHS

Health Sector Cybersecurity
Coordination Center

HC3: Sector Alert

June 07, 2024 TLP:CLEAR Report: 202406071200

Prevention of Unauthorized Access for Snowflake

Executive Summary

On June 02, 2024, Snowflake observed an increase in cyber threats targeting accounts on their cloud data platform. The vulnerability is possibly associated with [CVE-2023-51662](#). HC3 strongly encourages all users to review the following advisory, and to apply any mitigations to prevent serious damage from occurring to the Healthcare and Public Health (HPH) sector.

Report

Snowflake has recently detected and is investigating an uptick in cyber threats targeting certain customer accounts. The manufacturer suspects this is due to ongoing, industry-wide, identity-based attacks to access customer data. Additional research suggests that these attacks use user credentials that are exposed through unrelated cyber incidents. It is not believed that this activity is linked to any vulnerability, misconfiguration, or malicious activity within the Snowflake product, but may be related to CVE-2023-51662.

Detailed information on preventing any possible threat activity within Snowflake accounts and on disabling these malicious accounts can be viewed [here](#).



It should be noted that, if the ALLOW_ID_TOKEN parameter is enabled on your account, you must keep the user disabled for six hours to fully invalidate any potential unauthorized access through this ID token feature. Re-enabling the user before this period ends could allow an attacker to generate a new session using an existing ID token, even if the password has been reset or if MFA has been enabled. After deactivating the account, Snowflake recommends contacting the account owner to verify if the activity originated from them.

Snowflake is investigating activity from the following IP addresses:

• 104.223.91.28	• 146.70.117.56
• 198.54.135.99	• 169.150.201.25
• 184.147.100.29	• 66.63.167.147
• 146.70.117.210	• 194.230.144.126
• 198.54.130.153	• 146.70.165.227
• 169.150.203.22	• 154.47.30.137
• 185.156.46.163	• 154.47.30.150
• 146.70.171.99	• 96.44.191.140
• 206.217.206.108	• 146.70.166.176
• 45.86.221.146	• 198.44.136.56
• 193.32.126.233	• 176.123.6.193
• 87.249.134.11	• 192.252.212.60
• 66.115.189.247	• 173.44.63.112
• 104.129.24.124	• 37.19.210.34
• 146.70.171.112	• 37.19.210.21
• 198.54.135.67	• 185.213.155.241
• 146.70.124.216	• 198.44.136.82
• 45.134.142.200	• 93.115.0.49
• 206.217.205.49	• 204.152.216.105

[TLP:CLEAR, ID#202406071200, Page 1 of 5]

U.S. Department of Health and Human Services
Health Sector Cybersecurity Coordination Center (HC3) [www.HHS.GOV/HC3](#)



Office of
Information Security
Securing One HHS

Health Sector Cybersecurity
Coordination Center

HC3: Sector Alert

June 27, 2024 TLP:CLEAR Report: 202406271500

Critical MOVEit Vulnerabilities Expose Health Sector to Data Breaches

Executive Summary

A critical vulnerability has been identified in MOVEit, a common file transfer platform utilized in the health sector. This vulnerability exposes healthcare organizations to cyberattacks, especially ransomware and data breaches. Progress, the company that owns and operates the MOVEit platform, has released patches to fix this vulnerability. However, exploit code is also available to the public, and this vulnerability is being actively targeted by cyber threat actors. All healthcare organizations are strongly urged to identify any vulnerable instances of MOVEit that exist in their infrastructure and patch them as a high priority.

Analysis

Progress Software, an American business application company, identified and patched two improper authentication vulnerabilities in their MOVEit-managed file transfer (MFT) platform in early June 2024. These vulnerabilities are identical, other than the versions of the MOVEit platform that they affect. Both of them have been patched. (Please see the [Patches, Mitigations, and Workarounds](#) section below for specifics.) Shortly after the Progress security bulletins were released, WatchTower labs released [further research on one of them](#) – CVE-2024-5806 – which not only provided further details on the vulnerability, but also explored how it might be exploited. WatchTower also publicly released [proof-of-concept exploit code](#). The company Censys followed this up with [research in late June](#) noting that, at the time of publication, they were able to identify 2,700 vulnerable MOVEit MFT instances accessible from the Internet, most of which were physically located in the United States. These vulnerabilities – especially CVE-2024-5806 – should be taken seriously, as they are inherently egregious, but additionally, the MOVEit platform [has been previously targeted by highly-capable threat actors](#) on a [large scale](#).

Vulnerabilities

Progress Software identified and patched two vulnerabilities in their MOVEit-managed file transfer platform in early June 2024. These vulnerabilities are:

- [CVE-2024-5805](#) - Improper Authentication vulnerability in Progress' MOVEit Gateway that can allow for authentication bypass. This vulnerability impacts MOVEit Gateway: 2024.0.0.
- [CVE-2024-5806](#) - Improper Authentication vulnerability in Progress' MOVEit Gateway that can allow for authentication bypass. This vulnerability impacts MOVEit Transfer: from 2023.0.0 before 2023.0.11, from 2023.1.0 before 2023.1.6, from 2024.0.0 before 2024.0.2.

These vulnerabilities are identical, other than the versions of the platform they affect. Both of them have been patched. (Please see the [Patches, Mitigations, and Workarounds](#) section below for specifics.)

Patches, Mitigations, and Workarounds

The security bulletins, including patches for the two vulnerabilities, are located at each of these links:

- [MOVEit Gateway Critical Security Alert Bulletin – June 2024 – \(CVE-2024-5805\)](#)
- [MOVEit Transfer Critical Security Alert Bulletin – June 2024 – \(CVE-2024-5806\)](#)

These patches should be prioritized for deployment.

References

MOVEit Gateway Critical Security Alert Bulletin – June 2024 – (CVE-2024-5805)

[TLP:CLEAR, ID#202406271500, Page 1 of 2]

U.S. Department of Health and Human Services
Health Sector Cybersecurity Coordination Center (HC3) [www.HHS.GOV/HC3](#)

[202406041700_Baxter Welch Allyn Vulnerabilities Sector Alert_TLPCLEAR \(hhs.gov\)](#)

[202406071200_Snowflake Sector Alert_TLPCLEAR \(hhs.gov\)](#)

[202406271500_MOVEit Sector Alert_TLPCLEAR \(hhs.gov\)](#)

Addressing Current Threat Environment

Specific recommendations related to what was just discussed

- Mature your vulnerability management program
 - Move from periodic scans to continuous scanning
 - Establish capabilities to rapidly remediate or contain critical vulnerabilities
- Ensure MFA is in place for all public facing systems
- Ensure on-going monitoring of system activity to identify suspicious user behavior in EHRs
- Conduct or update your previous business impact analysis (BIA), with focus on impact of longer-term (weeks vs. days) unavailability of systems
- Update incident response plans to consider back-up procedures when a critical vendor is impacted by a ransomware attack
- Update your risk analysis to include all information systems with ePHI and/or that are critical to operations. Ensure risk analysis includes all potential vulnerability-threat scenarios, such as insider threats, credential compromises, and threats presented by third parties accessing your systems



Regulatory Update



OCR Enforcement: Heritage Valley Health System

Latest resolution agreement reaffirms OCR's focus on risk analysis and expectation of on-going, continuous risk analysis and risk response.

- OCR's third corrective action plan related to ransomware
- Failure to conduct a "compliant" risk analysis
- Failure to implement a contingency plan to address ransomware attacks
- Failure to implement policies and procedures limiting access to ePHI
- \$950,000 penalty and 3-year CAP

OCR States Its Expectations for Risk Analysis & Management

- 1. Must "integrate risk analysis and risk management into business processes"**
- 2. Must "conduct them regularly when new business operations and technologies are planned"**

Texas Federal Judge Rules OCR's Guidance on Online Tracking Technologies is Unlawful

Case 4:23-cv-01110-P Document 67 Filed 06/20/24 Page 1 of 31 PageID 1421

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION

AMERICAN HOSPITAL ASSOCIATION,
ET AL.,

Plaintiffs,

v.

No. 4:23-cv-01110-P

XAVIER BECERRA, ET AL.,

Defendants.

OPINION & ORDER

Before the Court are cross-motions for summary judgment. ECF Nos. 24, 50. Having considered the motions, briefs, and applicable law, the Court **GRANTS in part** and **DENIES in part** Plaintiffs' motion (ECF No. 24) and **DENIES** Defendants' motion (ECF No. 50).

BACKGROUND

Congress passed the Health Insurance Portability and Accountability Act ("HIPAA") in 1996 because health information needed more protections and the world needed more acronyms. HIPAA seeks to "assure that individuals' health information is properly protected" while "allowing the flow of health information needed to provide and promote high quality healthcare." The Department of Health and Human Services ("HHS") enforces this mandate. Violations are reported to HHS's Office for Civil Rights ("OCR"), who investigates reports and recommends corrective action. This case involves HIPAA's confidentiality protections (the "Privacy Rule") for "protected health information" ("PHI"). More specifically, the case concerns the Rule's applicability to one subset of PHI: "individually identifiable health information" ("IIHI"). HIPAA defines IIHI as information that (1) "relates to" an individual's healthcare and (2) "identifies the individual" or provides "a reasonable basis to believe that the information can be used to identify the individual."

The Court **GRANTS** the Hospitals' request for declaratory judgment and **DECLARES** that the Proscribed Combination, as set forth in the HHS Bulletin of March 18, 2024, is **UNLAWFUL**, as it was promulgated in clear excess of HHS's authority under HIPAA. *See La. Pub. Serv. Comm'n*, 476 U.S. at 374. While the Court **DENIES** the Hospitals' request for a permanent injunction, it **GRANTS** their request for vacatur and **ORDERS** that the Proscribed Combination be **VACATED**.⁸

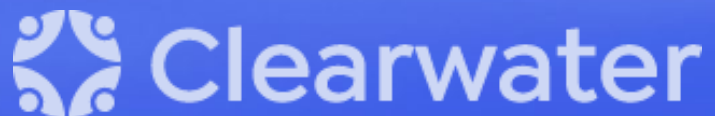
- The Court ruled that OCR's guidance was unlawful and that it had exceeded its power in expanding the definition of IIHI
- Denied request for permanent injunction
- Important to note that FTC and state privacy laws still apply

Compliance Recommendations

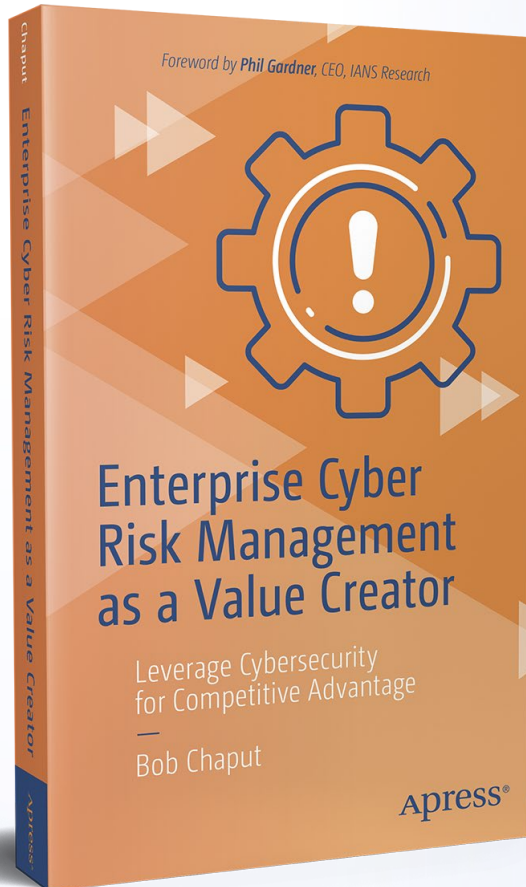
1. Complete Gap Assessments of HIPAA and state requirements
2. Migrate your risk analysis and risk management process from a once-a-year event to an on-going program
3. Update your risk analysis to include changes to technologies and operations
4. Document your risk management plan, and keep it updated
5. Make updates to policies and procedures
6. Prepare for Cybersecurity Performance Goals mandates – potentially coming in the next months or even weeks

Changing the Conversation about Cybersecurity in Healthcare

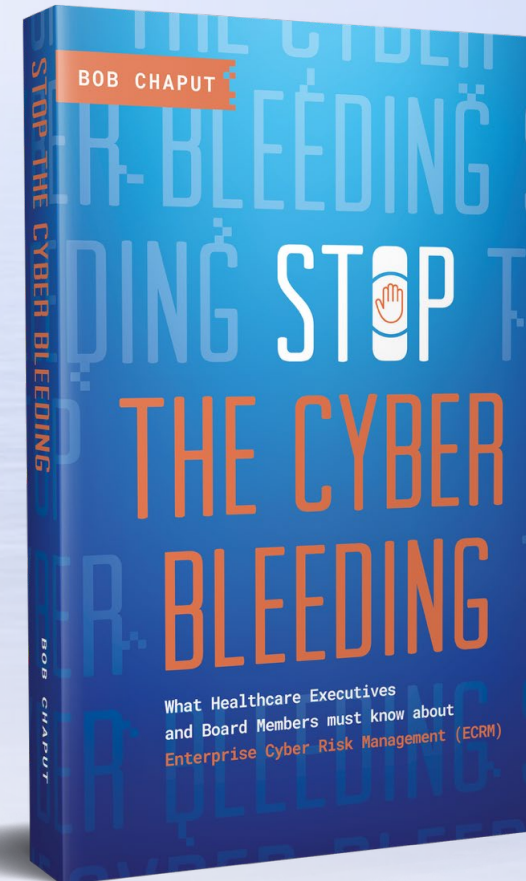
Steve Cagle and Bob Chaput



Related Resources



<https://amzn.to/3NYdafQ>



<https://amzn.to/3TLOqJR>

How well-aligned are your ECRM strategies and goals with your Business strategies and goals?

Access your complimentary *Business-ECRM Alignment Diagnostic* at

<https://bobchaput.com/alignmentdiagnostic/>


Bob Chaput

Business and Enterprise Cyber Risk Management (ECRM)

Alignment Diagnostic

INTRODUCTION

In this alignment diagnostic, you will develop an understanding of how well your enterprise cyber risk management (ECRM) and business goals align to help ensure that your ECRM program and cybersecurity strategy support your business strategy.





Q&A



Upcoming Webinars



The 405(d) Advantage: What Healthcare Leaders Should Know | July 18 @ 1:00 CST

[Register here](#)



Healthcare and the DoD: Preparing for CMMC Compliance | July 31 @ 12:00 CST

[Register here](#)



OCR-Quality® Risk Analysis Working Lab 2024: Beginning August 7th @ 11:00 am CT

[Register here](#)



We are here to help.

*Moving healthcare organizations to
a more secure, compliant, and
resilient state so they can achieve
their mission.*



Clearwater

Healthcare – Secure, Compliant, Resilient

www.ClearwaterSecurity.com

800.704.3394

LinkedIn | [linkedin.com/company/clearwater-security-llc/](https://www.linkedin.com/company/clearwater-security-llc/)



Legal Disclaimer

Although the information provided by Clearwater Security & Compliance LLC may be helpful in informing customers and others who have an interest in data privacy and security issues, it does not constitute legal advice. This information may be based in part on current federal law and is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource and should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS AND RECOMMENDATIONS PROVIDED BY CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

All materials contained within this document are protected by United States copyright law and may not be reproduced, distributed, transmitted, displayed, published, or broadcast without the prior, express written permission of Clearwater Security & Compliance LLC. You may not alter or remove any copyright or other notice from copies of this content.

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Security & Compliance LLC.