BUYING A BREACH

Security Considerations When Acquiring a New Healthcare Organization

scope

CONTENTS

Introduction 1

M & A Cybersecurity Challenges 3

Healthcare Acquisition Cybersecurity Playbook 7

- Timeline 8
- Phase One: Due Diligence 9
- Phase Two: Integration 12
- Phase Three: Post-Integration 19

Conclusion 20

About Scope Security 21

About the Author:

Mike Murray is the founder and CEO of Scope Security, the healthcare security company. At Scope, Murray builds on his nearly two decades of experience to solve critical security problems in healthcare.

Prior to founding Scope, Murray served as the Chief Security Officer at Lookout, where he presided over the protection of nearly 200m mobile users and their data. Previously, he led Product Development Security at GE Healthcare, where he built a global team to secure GE's portfolio of medical devices and services. Murray also co-founded The Hacker Academy and MAD Security, and has held leadership positions at companies including nCircle Network Security, Liberty Mutual Insurance and Neohapsis. He can be reached at mmurray@scopesecurity.com.

INTRODUCTION

NOW MORE THAN EVER, HEALTHCARE ACQUISITIONS REQUIRE A NEW LEVEL OF SECURITY DUE DILIGENCE. UNDERSTANDING THE HIDDEN RISKS AND HOW TO MITIGATE THEM CAN HELP AVOID TROUBLE DOWN THE ROAD.

The past few years have seen a significant rise in healthcare mergers and acquisition (M&A) activity. As fiscally sound providers continue to seize buying opportunities, it is crucial to fully evaluate the security health of the target organization - particularly as threats to this sector have increased significantly during the Covid-19 pandemic.

Getting cybersecurity right for M&A is hard, even during the best of times. The gold standard is to perform a comprehensive audit of policies, procedures and practices during the due diligence phase.

Figure 1. Number of Q2 Announced Transactions, by Year

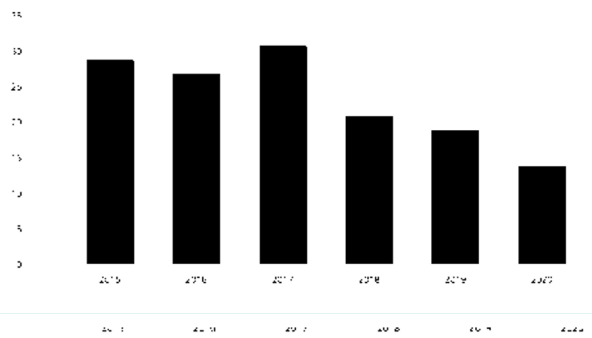
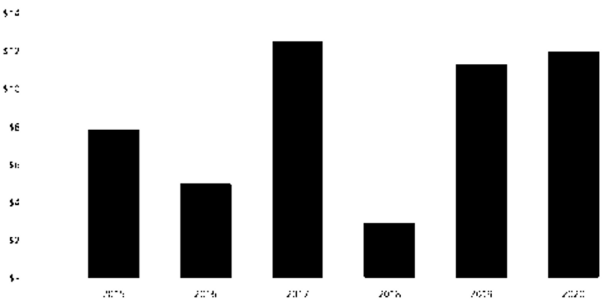


Figure 2. Total Q2 Transacted Revenue ($ in Billions), by Year



Source: Kaufman, Hall and Associates

Year over year activity has remained strong over the last five years. And while the number of deals in Q2 2020 are down from previous years, the amount of the transacted revenue increased, meaning larger organizations are joining forces. Early into the Covid-19 crisis, many in-progress M&A deals were put on hold or cancelled, but that could be changing. In its Q2 2020 Hospitals and Health Systems M&A report, industry analysts Kaufman, Hall noted that "the need to address COVID-19's impacts paused activity but did not change the underlying strategic rationale for many transactions; if anything, the pandemic may have strengthened the rationale for partnerships." And with the pandemic driving hospital losses into the billions, selling may be the only option. Analysts at investment bank Juniper Advisory, wrote that "the pandemic is creating a buyer's market in which stressed hospitals are forced to sell for much-needed cash infusions and other support to keep their doors open."

Increased M&A activity involving distressed assets means complex and high-risk security integrations, at a time when breaches are already exploding. In fact, healthcare was the most targeted industry in 2019, accounting for 382 breaches and costing over $2.45b.

INTRODUCTION

The nature of a data breach is that it lives undetected in the operational environment of the organization until it doesn't; this means that it is impossible to discover the breach during an audit of practices and policies. Similarly, even if the deal flow allows for (or the organization has recently performed) a comprehensive vulnerability assessment or penetration test, these offer only a picture of the state of vulnerability; rarely do these provide insight into which threats may be lurking under the. surface.

This danger exists in all M&A, but healthcare is at particular risk for acquiring a breach. First, because the due diligence process relies on the security maturity of the acquisition target, the healthcare industry suffers - over 85% of US hospitals and practices don't have any security resources on staff. This even further compromises the quality of due diligence and limits the confidence in the results from standard evaluation processes.

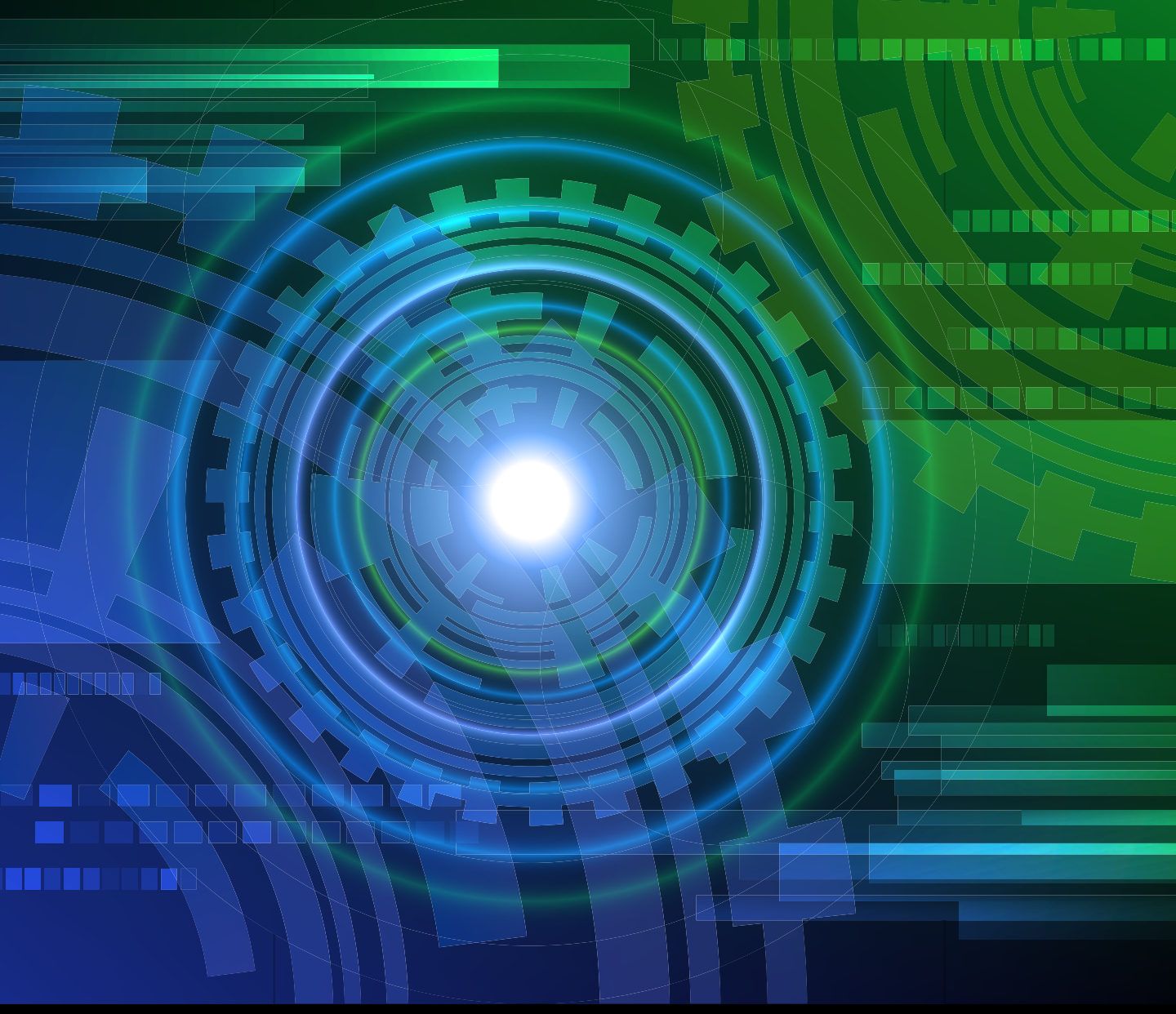
Second, and equally as important, the consequences of acquiring a breach can be much higher due to healthcare regulations and the unique characteristics of the healthcare delivery business model. While a breach is always costly for any organization, the diligence of HHS in investigating and fining offending organizations can be extremely costly, with settlements averaging nearly $1.8 million and total breach costs reaching $6.5 million. And these are just the hard costs of breach cleanup and fines - a 2019 Accenture study estimated that "each provider organization lost an average of $113 million of lifetime patient revenue for every data breach it suffered."

Since healthcare organizations often run at low margins, the acquisition of an organization that has an undetected breach could lead to cleanup costs, fines and lost revenue that are significantly higher than the anticipated profit from the acquisition, potentially meaning that the deal loses money over years. This is exactly the opposite of why the organization was acquired in the first place. Finally, healthcare can suffer most from the integration phase of the acquisition. While it can be expensive to acquire an undetected breach in a satellite organization, attackers rarely stop there. As the new organization is integrated into the acquiring organization, the networks will be linked together and systems connected. This allows the attacker who was quietly siphoning data from the acquired organization an opportunity to penetrate the larger system, potentially spreading the breach and magnifying its impact.

Hospitals account for 30% of all large healthcare breaches.

Source: The American Journal of Managed Care, 2018

Luckily, there are ways to blunt the impact of these challenges. While due diligence best practices are limited by the quality of the security program in the acquired organization and by the time and opportunity to engage with them, the integration phase offers opportunities to discover and corral the breach before it can cause significant damage to the acquiring organization. Especially key to mitigating and reducing this risk is the performance of a rapidly deployed and detailed threat hunt before any networks and systems are integrated together, and an ongoing monitoring program that focuses on any potential ingress points for threats to enter from the acquired organization.



M&A CYBERSECURITY CHALLENGES

In every industry, the costs of buying a breach are rising. Healthcare acquisitions come with a particular set of risks.

ACROSS INDUSTRIES, THERE CAN BE SIGNIFICANT RISKS IN ACQUIRING COMPANIES THAT HAVE INADEQUATE CYBERSECURITY MATURITY AND DISCIPLINE.

Acquiring a security breach can have massive operational and financial impact. The most high-profile example was seen during the acquisition of Yahoo! by Verizon. The discovery of a breach at Yahoo! during the acquisition process led to a renegotiation of $350M (approximately 10%) off the originally negotiated purchase price. This doesn't even include the costs to Yahoo! of handling and managing the situation.

Traditionally, one of the main obstacles to uncovering these breaches is the difficulty of performing adequate security due diligence during the acquisition process. While an analysis of the financial health of the business can be detected by running the appropriate level of (audited) financial reporting, there is no easy way to discover a data breach from the reports generated around security risk.

In a seller's market, the due diligence process has usually limited security access to an on-paper audit of the new acquisition's security program, policies and procedures, and architecture. It has rarely allowed deeper vulnerability scans and penetration testing and almost never access for detailed threat hunting.

While that level of due diligence can provide some clues, it doesn't give a good indication that an undiscovered breach is lying in wait, as these reports indicate only what is known about the environment. Only a strong view into the day-to-day operations of security can provide around finding anomalies that point to undiscovered conditions can provide that indication. That level of diligence has not traditionally been possible before an acquisition closes, because of the access required.

A MergerMarket study found that more than 80% of acquirers reported finding breaches in more than 25% of their targets post-acquisition. And the Wall Street Journal reported that 66% of acquisitions in 2018 failed, "39% [pointing] to "concerns about cybersecurity."

New market conditions (especially when acquiring a distressed practice) may allow a more permissive environment. Where we have traditionally be limited to the paper audit, acquiring organizations should require that the acquisition target deploy a rapid threat hunting solution in advance of the deal closing. This can provide strong assurance that the purchase price and deal model reflect any possibility of buying a breach.

THE RISK OF BUYING A BREACH INCREASES IN HEALTHCARE. MOST ORGANIZATIONS DON'T HAVE THE STAFF OR BUDGET TO RUN A COMPREHENSIVE SECURITY PROGRAM - EVEN THOUGH HEALTHCARE IS THE MOST TARGETED INDUSTRY.

Upon closing, there is often a push to integrate the newly acquired organization into the day to day operations of the acquiring organization; this includes integration of networks to allow sharing of data, integration of identity management so that have accounts in the acquiring organization, and integration of data and service delivery (including EHR systems, billing cycle management, etc).

Larger acquiring organizations will usually have a mature security program and will be able to perform some due diligence. However,due diligence traditionally relies the quality of the target's security organization. When 85% of the acquisition targets don't have even a single qualified security person, it diminishes the quality of due diligence and increases the potential of inheriting a hospital that has significant security issues..

What is even worse: if the acquired healthcare organization is distressed (from those struggling all the way to those who have declared bankruptcy), these issues will be exacerbated.

High risk procedure: Why healthcare M&A poses unique security challenges

- According to HHS, 85% of US healthcare organizations don't have qualified security teams
- Medical and clinical technology often run very outdated and vulnerable software
- Security solutions often don't have visibility into the main asset base and threat surface (ie, EMR, medical devices & back-office infrastructure)
- Targets often have patchwork architecture built from their own series of roll-ups or acquisitions
- Cybersecurity budgets and staff are often constrained

These organizations will likely have reduced their spending on network and system modernization and security even more as they attempt to stay afloat long enough to be acquired.

Observing the limited data about hospital acquisitions, this exact pattern plays out. A 2018 study from West Monroe Partners revealed that 58 percent of healthcare buyers discovered a cybersecurity problem at an acquired healthcare company after the deal was done. This is a significant amount of acquired risk, and it can lead to huge headaches down the road.

This can get expensive quickly. The average healthcare breach costs around $6.5 million, significantly higher than most other industries. And with median operating margins running in the 1-2% range, the cost of cleaning up the breach that is discovered post acquisition can rapidly wipe out most or all of the expected profits of the acquisition for multiple years.

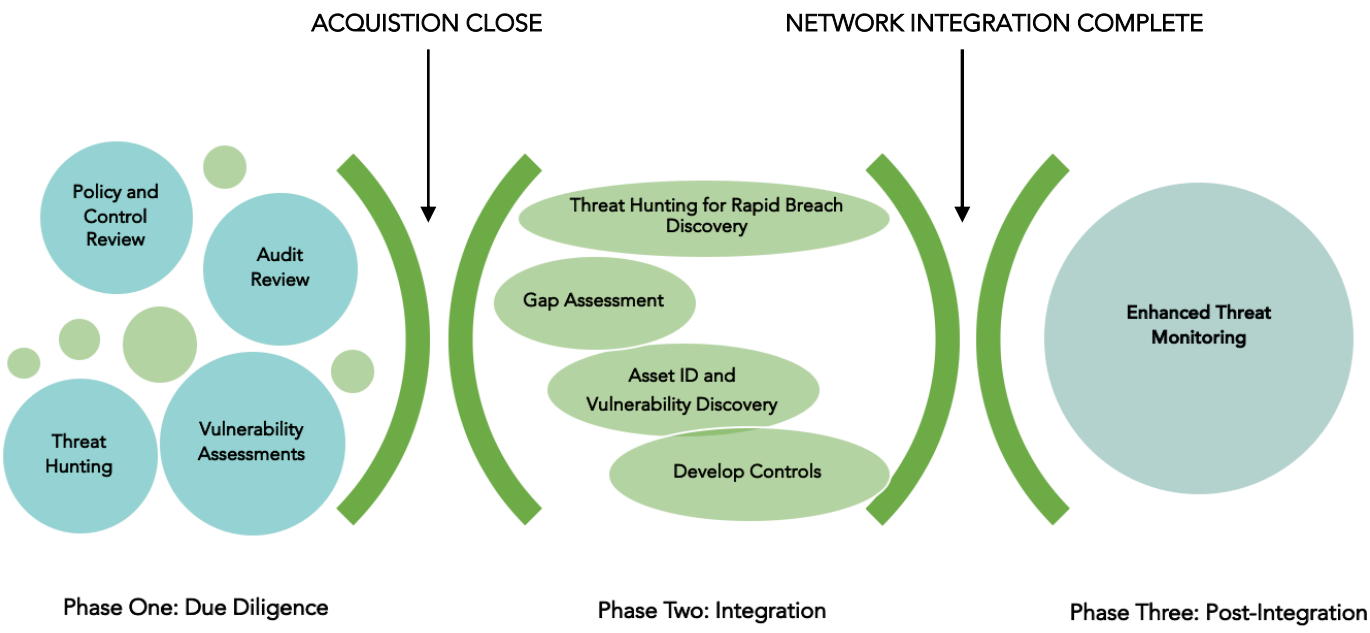
This is exactly the opposite of why the organization was acquired in the first place. This is before we even calculate the loss of brand equity and reputation to the acquiring organization. A Ponemon study found that 50% of patients said they would find a different provider if they were not confident in their healthcare providers' security practices. This led Accenture to conclude that each provider organization that suffers a breach will lose an average of $113 million of lifetime patient revenue.

Ultimately, this shows that purchasing a provider that has an undiscovered data breach could have deleterious effects to the acquiring organization that last for years to come.

HEALTHCARE ACQUISITION CYBERSECURITY PLAYBOOK

What to look for during each phase of the M&A process, from due diligence to post-integration.

THE THREE PHASES: A TIMELINE OF ACTIONS YOU MUST TAKE TO AVOID BUYING A BREACH



Any acquisition involves multiple teams, workstreams, checkpoints and sign offs. This guide is intended to highlight only the most critical activities in order to understand the cybersecurity posture of the hospital, clinic or healthcare organization you are acquiring, and to uncover any potential landmines. Many of the steps within these phases overlap; in particular during the integration phase it is important to note that threat hunting is continuous across the Integration phase of the acquisition.

PHASE ONE: DUE DILIGENCE

IN THIS PHASE:

- POLICY AND CONTROL REVIEW
- AUDIT REVIEW
- VULNERABILITY ASSESSMENTS
- THREAT HUNTING

The work of the cybersecurity organization in the acquiring hospital starts during the Due Diligence phase of the acquisition, and the hope is that this process enables the organization to quantify its risk in acquiring the new provider. This phase usually involves an audit of the new practice's security program, including any audits that they have had done, their policies and procedures, etc. These audits are a blunt tool that can often be enough to identify if the organization has done a bare minimum of security due diligence - for example, if the organization previously had a breach that was reported in the news or to OCR, if they don't have a security team, or if their audits show significant and obvious gaps, then it is clear that they are taking on significant unmanaged and unquantified risk.

But it's not usually that simple. If it were, the statistics would show a much higher success rate. The previously mentioned West Monroe Partners study showed that 49 percent of buyers reported dissatisfaction with the cyber due diligence process during the deal. This tells us that the information that is truly needed to make a solid risk quantification can't be obtained through the traditional due diligence process (i.e. paper audits or even vulnerability scans) .

49% of buyers reported dissatisfaction with the cyber due diligence process during the deal

Source: West Monroe Partners. "Reshaping Healthcare M&A," 2018

In fact, it is the unseen risk (that is not described in the audit reports, policies and procedures) that ultimately makes acquisitions difficult. That's not to say that traditional due diligence isn't worth doing - it can help inform the potential security resources required once the acquisition is closed. And it can help quantify the magnitude of "unknown unknowns" that are lurking to be discovered during the transition.

Because of this challenge, it is worth at least attempting to require the target organization to deploy rapid threat hunting (as we prescribe for the integration phase) as part of the due diligence process – this may not always be possible, but it significantly reduces the risk of acquiring a security breach in progress.

MODERN DUE DILIGENCE BEST PRACTICES FOR HEALTHCARE M&A

At a foundational level, the security due diligence process should include:

1. Reviewing the target organization's security program, policies and procedures to determine their level of **security maturity and discipline,** including with respect to organizational (policies), operational (processes), and technical controls

2. Understanding the **network and system architecture and data flows**, including the use of cloud providers and third-party applications and where security controls are located

3. Understanding where **PHI is located** and how it flows through the environment

4. **Threat modeling** of the above data flows and understanding the control environment as it is documented to determine if key threat vectors (e.g. data exfiltration from the EMR) are covered

5. Determining whether the selling entity has experienced **any prior cybersecurity incidents,** including reported or unreported data breaches, and how it has responded to such incidents

6. Reviewing recent **vulnerability assessments**, penetration tests and asset inventories, especially with a focus on potential open threat vectors that could indicate opportunities for data breaches to go unnoticed

7. If the deal timeline and structure allows, performing of additional vulnerability assessments and research of open-source information (e.g. Shodan) to gain a current understanding of the **attack surface of the organization**

8. If possible, require the target organization to deploy rapid threat hunting (as described in the integration phase on pg. 17) during the due diligence process and report 30 days of results before the deal closes. This is the most significant method to reduce the risk of acquiring a breach as it happens.

PHASE TWO: INTEGRATION

IN THIS PHASE:

- GAP ASSESSMENT
- ASSEST ID AND VULNERABILITY DISCOVERY
- DEVELOP CONTROLS
- THREAT HUNTING FOR RAPID BREACH DISCOVERY

Once the acquisition has closed, the next step is to integrate the newly acquired practice into the acquiring system's environment. This includes connections between the two organizations' networks, the transition of their users to accounts that allow access to shared resources, and the connection of medical infrastructure like EMRs to allow shared workflow between the medical environments.

That integration is the point at which an undiscovered breach presents the most risk for the acquiring organization: once the environments are connected together, an attacker hiding in the acquired provider can start to attack the environment of the acquiring system, and the breach can spread and expand. One of the worst case scenarios for any acquisition is to integrate with the newly purchased asset only to discover that the integration enabled lateral movement for an attacker that is already living in the newly acquired environment.

Fortunately, it is possible to structure cybersecurity activities during the Integration phase of the acquisition to maximize the likelihood of discovery of any breaches, and minimize the risk of integrating networks, user identities and medical infrastructure as the acquisition progresses.

The integration process has four key steps that extend from the moment that the deal closes to the point at which technical and business integration is complete:

1. Detailed Gap Analysis
2. Security Architecture/Control Deployment
3. Human & Technology Vulnerability Assessments
4. Rapid Breach Discovery Through Detailed and Dedicated Threat Hunting

CONDUCT A DETAILED GAP ASSESSMENT

The due diligence phase of the acquisition already provided a review of the new organization's policy and infosec program. However, where that review was focused on evaluating the maturity of the program to give a directional assessment of risk to help value the acquired organization, this review requires a more critical assessment of the gaps between the processes, procedures and operations of the way that the acquired organization manages its security program against the standards of the acquiring one. The goal of this assessment is ultimately to create a worklist for the integration between the two environments by determining what parts of their policies and program align and what needs to change.

Often, these changes are little more than cosmetic; small changes in wording between the two organizations' business continuity plans, for instance, can be brought into alignment easily. But often this assessment may find issues that are more difficult to address, especially if those changes touch the users of the acquired organization.

In 2019, the average total cost of a data breach in the healthcare industry was $6.45 million, or 65% higher than the average total cost of a data breach.

Source: IBM 2020 Cost of a Data Breach Report

One of the most insidious examples of these is password policies: a roll out of a new password policy to the acquired acquisition can create friction for the medical and administrative staff of the organization and cause consternation as part of the acquisition. These changes need to be planned and implemented thoughtfully to create the best alignment between the acquired organization and the acquiring one.

Additionally, the gap assessment needs to focus on the alignment of the control infrastructure in the newly acquired organization - specifically, to answer the question of whether security controls are deployed in a way that conforms to the standards of the acquiring organization.

GAP ASSESSMENT , CON'T

This involves reviews of:

- Technical Control Compatibility: what security control technologies are the two organizations using? Examples include log management and/or SIEM, threat detection (SOC/MSSP/MDR), authentication/access control, network security controls like firewalls and intrusion detection, data loss prevention (DLP), vulnerability scanners, phishing simulations, etc. Are the controls that the acquired organization uses compatible with and at a similar level of operational capability as the control environment of the acquiring one?

- Configuration and Enforcement Compatibility: Even if the technologies are compatible, their configurations may not be. As an example, the acquired organization may allow all outbound traffic through their firewall, while the acquiring one may restrict use. Or there may be a mismatch with the types of information that is permitted to be exchanged through email by DLP controls. Examine the configurations of the key security controls and ensure that expectations match around what will be permitted, what will be denied and what will be alerted on.

Special Considerations around Users and Identity Management: Identity management deserves specific focus. Policies and procedures around account privileges, privileged users and permissions across the organization can be where enormous gaps exist and where threats can slip through. Additionally, because these controls touch users, large headaches can exist when users are transitioning from a particularly permissive environment to a more locked down one. It can be frustrating for the security team of the acquiring organization if they gain the reputation as stopping the newly acquired organization from working, and usually that happens due to the way gaps are closed in user permissions.

Note that this review may create a long list of gaps between the two environments, especially in the acquisition of distressed assets who have reduced their investment in security maturity. The work-list that comes out of this phase may be daunting. It is important to prioritize control deployment activities that have the most "bang for the buck", as security does not often get to be the long pole in the tent on the integration timeline.

CONTROL DEVELOPMENT AND DEPLOYMENT

Once the list is created and prioritized, it is time to begin to perform integration activities in the acquired environment. This includes any architecture changes that are required, control technologies that need to be deployed, replaced or reconfigured and plans for changes in the identity and access control environment.

This is when the two organizations' IT, Security, Privacy and Biomedical/Clinical Technology organizations will really start to interact and work together. Remember, this is a stressful time for the teams on the acquired side of the transition, and they will require additional support and guidance to learn the acquiring organization's daily operating rhythms and ways of thinking.

During this phase, the acquiring company can make working with their colleagues at the acquired organization easy or challenging. This is especially true when the gap list requires that those at the acquired organization perform activities, change configurations or conform to new standards or ways of working. Time taken to ensure that those teams are aligned with (or at least understand) the decisions that have been made and the changes being implemented can make all the difference in the success of working together through, (and long after) the integration.

ASSET IDENTIFICATION AND VULNERABILITY DISCOVERY

The next step in integration is to have a detailed picture of the attack surface and vulnerability posture of the newly acquired environment. This calls for the use of vulnerability assessment tools to prioritize what needs to be fixed before the systems are integrated. If the organization is already doing a good job of asset inventory and vulnerability management, this may be as simple as reviewing the reports from the tools that they're using. If not, however, this step will likely involve setting up internal scanning infrastructure to match what the acquiring organization is using.

Some of the discovered vulnerabilities may demand immediate investigation and remediation, especially if the acquired organization has not focused on vulnerability and patch management. There may be severe vulnerabilities in important parts of the organization that are obvious priorities for remediation.

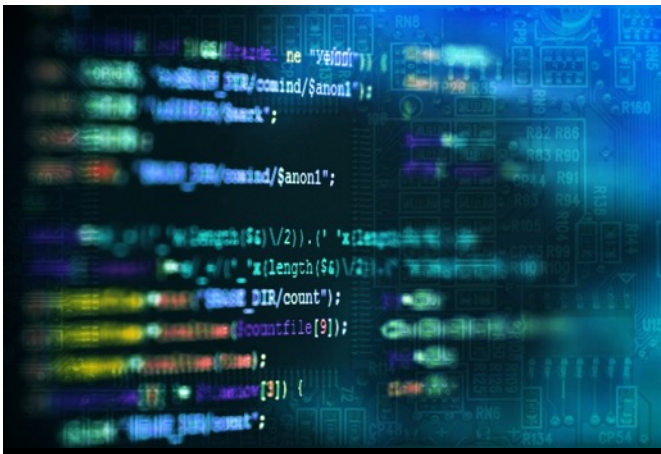
Unfortunately, this step of the integration process can create a huge list of potential vulnerabilities in the new organization. This may be especially true across parts of the environment that may not have been subject to the security discipline and configuration management of the standard IT systems (e.g. medical devices & other clinical technology). While this list can be somewhat daunting, it is key to prioritize three main types of assets and vulnerabilities that can:

- Allow uncontrolled ingress into the newly acquired organization
- Provide an attacker access to key information and systems, both from the perspective of data to be stolen as well as data that could be compromised in the event of a ransomware event.
- Provide an attacker the ability to easily pivot in to the acquiring organization once integration is complete.

Importantly, as soon as vulnerabilities are discovered, they should be passed to the team that is doing Threat Hunting (described in the next section) to assist them in narrowing down potential access and pivot points.

RAPID BREACH DISCOVERY

As discussed, the hardest thing to get a sense of during due diligence is the extent to which the acquired organization may already be compromised. At the same time, this is the highest risk that the acquiring organization faces in integration - that they may have purchased a breach in progress that is about to penetrate their organization. This will be especially true when the plan calls for the integration of identity management and endpoints - employees of the organization whose devices and credentials are compromised through phishing or other means can become a fast track into the acquiring organization's infrastructure.



Healthcare was the most targeted industry in 2019, accounting for 43% of breaches.

Source: ForgeRock 2020 Consumer Identity Report

For this reason, one of the most important parts of the transition phase is to kick off a threat hunting operation in the newly acquired environment. Ideally, this activity will last for 60-90 days and provide a full picture of the operational security environment and root out any potential latent threats that exist there. Because of the relatively long timeline that this requires, this step needs to be performed in parallel with all of the other integration activities.

This critical step may be hindered by two key limitations: first, the acquired organization's lack of deployed security tooling may make it difficult to acquire signal for threat hunting (especially in organizations that have traditionally underinvested in security); and second, few beyond the largest healthcare organizations have enough security resources to deploy a separate operations team to perform this work without impacting the security of the acquiring organization.

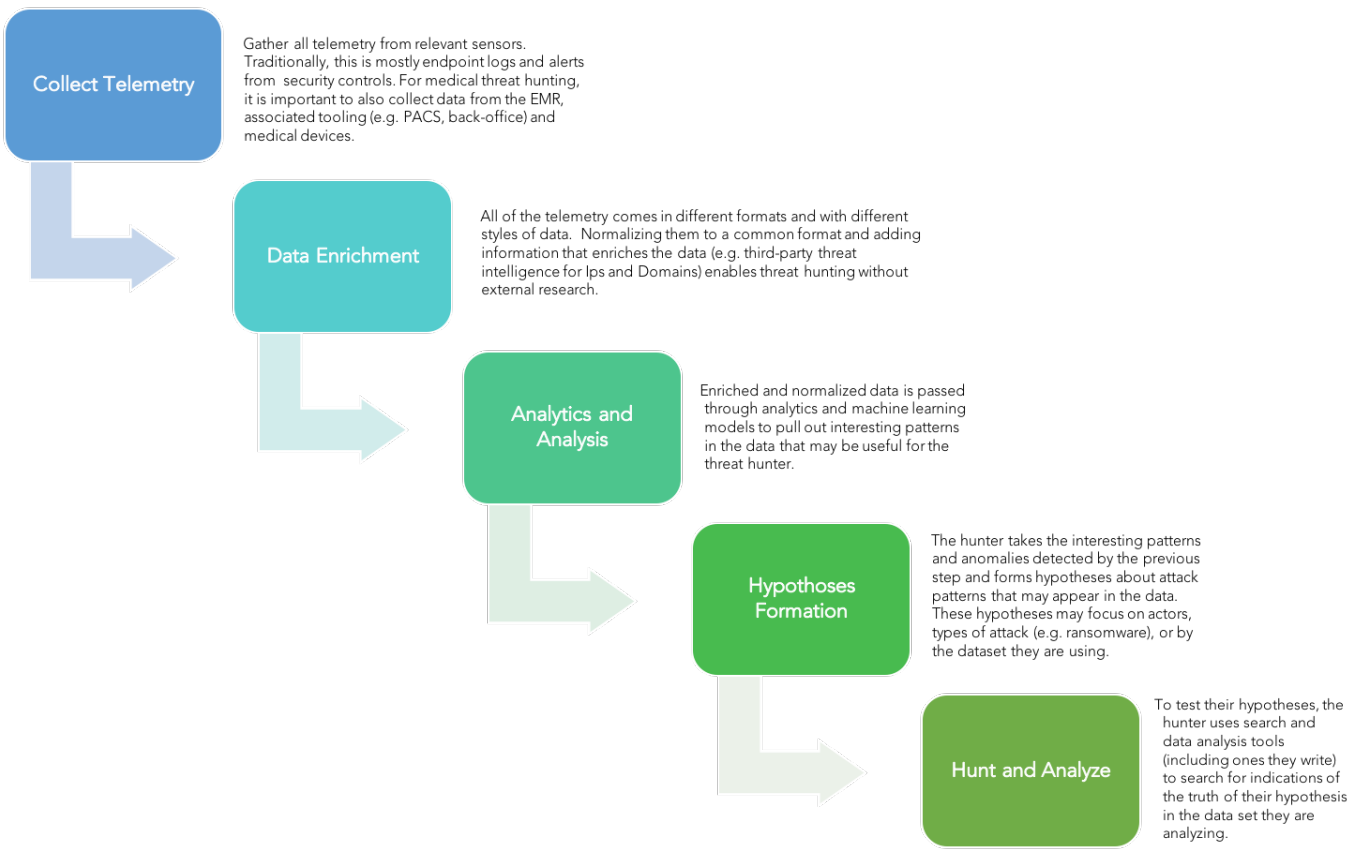
For these reasons, rapid deployment of a managed security service who can help get a picture of the actual operational environment is advised as a way to overcome the resource limitations.

RAPID BREACH DISCOVERY

While many managed security vendors aren't set up for this type of rapid, short-term engagement, there are modern products like Scope Security that can be deployed quickly and obtain signal for threat hunting across their network, security and medical infrastructure in an extremely short period of time. Rolling out this type of service ensures that threat hunting is performed thoroughly by a qualified team that can provide the visibility that would be lacking until complete control deployment and integration is accomplished.

This is especially important if the acquired organization has old, outdated or missing security controls - which is a fairly common scenario across healthcare. As discussed previously, the amount of work to deploy controls in legacy environments can take significant time (and often extends beyond the time of the integration of the newly acquired organization). Waiting until all controls are deployed to discover a breach can create significant gaps in the visibility needed to know that integration of networks and user identities carries an acceptable level of risk.

THREAT HUNTING: HOW TO FIND THE BREACH BEFORE YOU BUY IT



PHASE THREE: POST-INTEGRATION

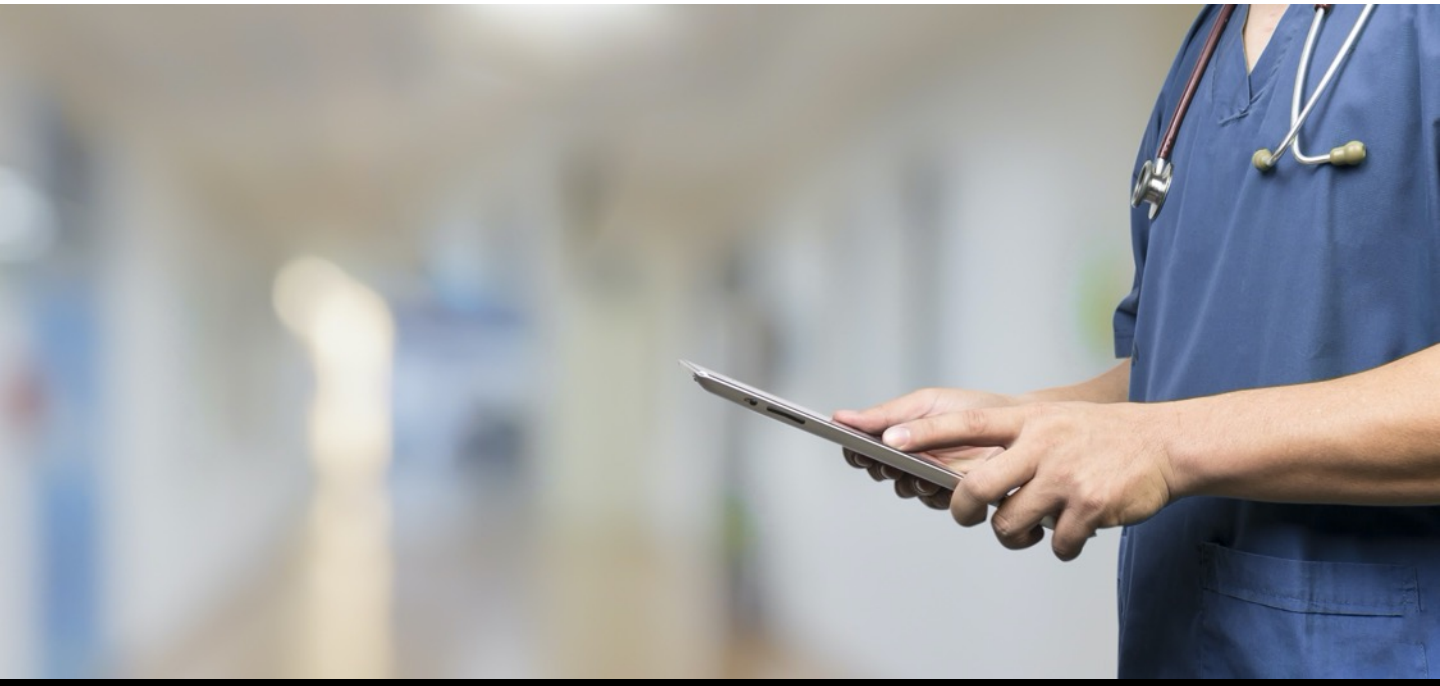
IN THIS PHASE:

- ENHANCED THREAT MONITORING

Once the integration is complete, a key step will be to continue to monitor the integration points of the newly-merged organization to ensure continued vigilance. While threat hunting and other pre-integration activities should have discovered any important threats lurking in the environment, continued diligence is needed. This is especially true if there were large gaps between the security practices and effectiveness of the acquired organization.

For example, suppose that the acquired organization failed to perform detailed phishing simulations over the years before the acquisition. Even if the new organization starts to test and train those employees going forward, phishing attacks will still be more successful against those employees than against the general population of the acquirer. Monitoring of those users' endpoints and account security becomes even more vital once the integration of the networks has been achieved, as those users are a vulnerability that can lead to increased compromises down the road.

This means that extra monitoring is needed for some amount of time around parts of the control environment that could still harbor gaps or be easier entry points for attackers. Understanding these gaps (in the security controls around networks, identities and medical infrastructure) and continuing to have strong and sensitive monitoring around them is key to ensuring that the newly acquired environment doesn't continue to provide entry points in the future.



CONCLUSION

Many healthcare organizations are taking advantage of the current and recent financial environment to snatch up troubled hospitals, clinics and other healthcare organizations. Even before the COVID-19 epidemic, which left many HDOs struggling financially, sector M&A activity was rising fast. The business case seems obvious, but when the potential for buying a hospital with a compromised security posture is factored in, the ROI on an acquisition can be significantly less appealing - or even turn negative.

When data breaches at the acquired hospital are discovered post-acquisition, it is too late to turn back. However, if the acquiring organization follows a disciplined playbook of security-focused due diligence, including detailed and focused threat hunting, many of these land mines will be uncovered early. This allows for the acquiring organization to adjust purchase or other terms accordingly, if necessary, and put in place a solid plan to address any breaches before integration. This also ensures that any previous penetration by bad actors is stopped at the border of the acquiring HDO's systems, keeping their security posture intact and minimizing the impact of any issues.

About Scope Security

Scope provides managed detection and response to protect hospitals, clinics and large provider systems from cyberattacks. We have custom-built our integrated technology and service platform to enable us to detect the complex attacks that healthcare organizations are facing across their entire technology landscape.

Scope monitors every aspect of today's increasingly connected healthcare environment—from traditional IT infrastructure to EMRs to medical devices—in order to detect advanced threats, protect patient data and keep healthcare organizations running. Our innovative solution delivers these detections and insights through a single, integrated view of your entire organization, to stop breaches before they compromise other systems in your network.

Scope is founded by experienced healthcare and security leaders who understand the unique challenges of securing health systems and is backed by leading venture capital firms, including Thrive Capital. We are a mission-driven company which believes that by protecting healthcare organizations from cyberattacks, we help protect the health and lives of their patients.

To learn more about who we are and how we can help you, please contact us at info@scopesecurity.com.