WHITE PAPER

IDENTITY FOR THE CISO NOT YET PAYING ATTENTION TO IDENTITY

H-ISAC™
HEALTH - ISAC

IDENTITY FOR THE CISO NOT YET PAYING ATTENTION TO IDENTITY

In many healthcare organizations, the CISO does not own the identity function. *Do you?*

You may be thinking, "I can't *own* identity, I have too many problems to solve already. My team doesn't provision accounts – that's IT. My team doesn't onboard employees – that's HR. My team doesn't manage customer relationships – that's Sales or Product."

In this paper, you will hear the case for why CISOs are starting to change their mindset on their role in identity and simple things you can do to start to shift your thinking.

INTRODUCTION

In cybersecurity, identity is suddenly more important than ever before.

How Business Operates Has Fundamentally Changed

Continuous technological evolution coupled with organizational shifts have fundamentally changed the way we operate our businesses. Cloud computing, mobile, IoT, and a dispersed and often remote workforce offer significant opportunities to those that can harness their capabilities. Beyond the enterprise, customers increasingly expect the ability to engage in an array of high risk, high value transactions from any device and location.

Previous Defenses Are No Longer Sufficient

This shift in how businesses operate has exposed the limitations of traditional cybersecurity approaches based on perimeter defenses. Increasingly, attackers are slicing through these defenses by focusing on exploiting weaknesses in identity – bypassing the "castle walls" of perimeter defenses by simply walking through the "front door" – with stolen or compromised credentials. Today, it is an anomaly when a major breach is announced and identity did not provide the attack vector.

The threat is particularly acute in healthcare, given the high value stolen health records fetch on the open market, as well as complex requirements for patients to access and transfer sensitive data.

Identity is at the Core of Protecting the Business

Adjusting to these new threat vectors requires not just better identity defenses – it requires a broader rethinking of traditional security models. An identity-centric approach to security better aligns resources to threat.

Healthcare CISOs are uniquely positioned to drive an identity-centric transformation in their organizations – both to improve security, but also to better serve customers and develop competitive advantages.

KEY TAKEAWAYS

1. Identity matters. It's where attackers increasingly focus, making it imperative that defenses are oriented around identity. With the explosion of cloud, mobile, and BYOD, organizations have reduced control of their endpoints, elevating the importance of identity.

2. Identity is not just about internal workforce; it's about an organization's entire ecosystem including customers and external partners.

3. Identity should be owned and operated by an organizational function motivated by risk (e.g., the CISO), not one motivated by service levels and speed (e.g., the Service Desk or HR).

4. CISOs should use an identity-centric approach to cybersecurity.

WHY IDENTITY MATTERS

Identity is the leading cause of breaches today. As the chart below details, if your organization is targeted, attackers are likely to start with attacks on identity systems – and if breached, the most likely source is exploitation of weaknesses in identity systems.

Typically, there are two elements to modern data breaches: First, a compromised password is used to establish access to a system. And second, attackers (both external and insiders) exploit inadequate Identity and Access Management (IAM) controls to access data that should be restricted – often in combination with escalation of privilege – allowing them to exfiltrate sensitive data.

Identity presents particular challenges in the health sector, given both the value of health data on the open market relative to other types of data[13], as well as the fact that access to consumer health data has to be managed by both enterprise and customer-facing systems.

Please see chart on next page ▶

WHY IDENTITY MATTERS

(Continued)

INCIDENT	DATE	CAUSE	FALLOUT
Yahoo	August 2013	Phishing and poor password management	~3 Billion accounts impacted; $117.5 million settlement cost[1]
Target	November 2013	Stolen credentials & unnecessary 3rd party access/permissions	$18.5 million in fines, 60 million customers impacted. CEO and other executives fired[2]
Anthem	February 2014	Compromised Admin account & lack of MFA and PAM	78.8 million individuals impacted; $260 million spent on security-related measures, lawsuits, and credit protection[3]
Heartbleed	April 2014	Bug that exposed passwords	Blamed for hundreds of stolen social insurance numbers in Canada[4] and stolen data from 4.5 million patients in the United States[5]
Sony	November 2014	Phishing and poor password management	~$100 million in legal and clean-up costs;[6] 46,800 contractors and employees were exposed to identity theft[7]
IRS	May 2015	Compromise of "Knowledge-Based" Authentication (KBA)	Tax data stolen from more than 700,000 Americans[8]
OPM	November 2015	Lack of MFA; compromised credential from a 3rd party vendor	Damage to national security; costs in excess of $1 Billion, 21M people impacted; Executives fired[9]
Democratic National Committee (DNC)	July 2016	Stolen (phished) credentials	Over $1 million in clean-up costs; political and reputational damage[10]
Uber	November 2016	Unsecured credential information & weak access controls	57 million accounts impacted; $148 million settlement cost[11]
Equifax	July 2017	Unsecured passwords, accessed after an initial patch management error provided a beachhead	148 million people impacted; CEO and other executives fired. ~$2.1 Billion in costs[12]

WHAT IS IAM?

Identity and Access Management (IAM) is the discipline, framework, technologies, and functions that relate to ensuring only the right individuals can access the appropriate resources at the appropriate time via the appropriate device for their approved tasks. Identity involves the creation and governance of digital identities within a system throughout their lifecycle. Access Management involves the technologies and processes that act in real time to monitor and control access by those digital identities.

IAM includes processes like provisioning and de-provisioning, authentication, authorization, verification, and the escalation or de-escalation of privileges. Common IAM solutions generally fit into one of the "6 As" outlined below —and may be delivered on premises or via the cloud.

Authentication

- Enabling users to prove they are whom they claim to be – via multiple factors, so that the compromise of one factor does not enable access

Access

- Ensuring that users, once authenticated, can easily access the right applications and resources (SSO)
- Prevent unauthorized users from gaining access
- Implementing additional controls for privileged users (PAM)

Authorization

- Ensuring that users are tightly governed in what they can access and do
- How are permissions or delegations granted or revoked?

Analytics

- Detecting whether identities are being used improperly or suspiciously – and triggering additional, appropriate controls

Audit

- Looking back to review events and confirm the identity system was being used properly
- Determining what happened if it was not

Administration

- How is the identity system governed?
- How are the policies and processes of the identity system managed?
- How are new identities added or removed from the system?

IDENTITY IS NOT JUST ABOUT THE INTERNAL WORKFORCE

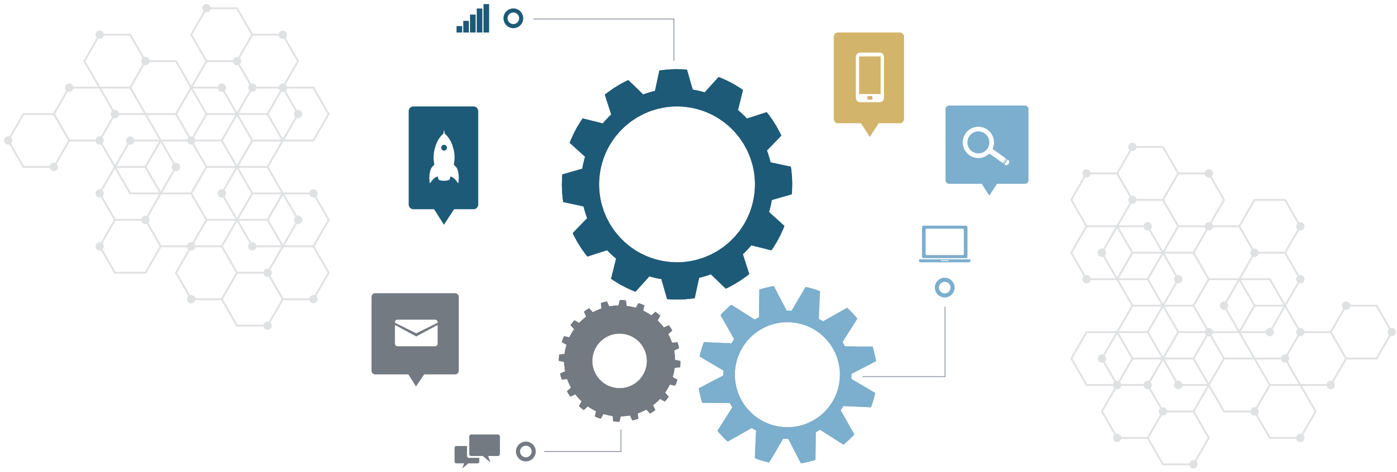
IAM is not a one-size-fits-all approach. Enterprise IAM solutions designed to manage the workforce are generally not suitable for an organization's customers, and vice versa – though there are some vendors focused on creating product suites that can cover requirements in both worlds. Additionally, IAM solutions are becoming increasingly important in the IoT space.

Enterprise IAM solutions

Enterprise IAM solutions are focused on managing access to different IT systems and data stores. Governance tends to be particularly important in enterprise solutions, given that an individual's roles and access rights tend to change over the years. Modern enterprise IAM solutions place an increasing emphasis on managing and controlling privileged users, who have the ability to access an organization's most sensitive and critical systems and data. Here, user experience is often secondary to security controls and corporate policies – though that is changing as vendors look to address issues with deployment friction and make it easier for employees and partners to get work done.

Customer IAM (CIAM) solutions

Customer IAM (CIAM) solutions tend to be designed with the user experience front and center – the idea being to eliminate friction and maximize the consumer experience. Most CIAM solutions require consumers to register themselves, which means that users are generally unknown when they first interface with the solution. Many health applications require that a CIAM solution can "identity proof" a user before granting access. CIAM solutions must also be built with scalability in mind. CIAM systems must be able to operate under heavy loads and accommodate tens or hundreds of millions of users. CIAM solutions often also prioritize extensive data collection and analytics tools to aide in marketing, business intelligence, and overall strategy. The way in which CIAM solutions address these latter functions are being materially impacted by new privacy laws and regulations such as Europe's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).



WHAT THREATS CAN AN IDENTITY-CENTRIC APPROACH TO SECURITY ADDRESS?

EXTERNAL THREATS

- Phished or Stolen Credentials
- Password Reuse and Sharing
- Privilege Escalation
- Customer Identity Compromise (ID theft)
- Brute Force Credential Attacks

INTERNAL THREATS

- Malicious Insiders
- Over-privileged Users/No Review & Revocation of Entitlements
- "Ghost Accounts" of ex-Employees Still Active
- 3rd Parties with Access to Enterprise Systems

An identity-centric approach to security can guard against internal and external threats alike. By making IAM a priority, organizations can guard against external threats that make use of stolen or compromised credentials that are often obtained by phishing scams. Robust IAM tools are also essential to guarding against insider threats related to privilege abuse. This is significant in light of statistics from the *Verizon Data Breach Investigations Report (DBIR)* showing that "healthcare stands out due to the majority of breaches being associated with internal actors."[14]

Data from the DBIR further illustrates how prevalent and serious these threats are, regardless of industry. In 2017, 81% of breaches involved weak or stolen passwords.[15] In 2018, stolen credentials and privilege abuse were ranked as the number one and number four attack vector in breaches.[16] Privilege misuse has represented the most common incident classification since 2014.[17] In 2019, 34% of breaches involved internal actors, a number which has increased since 2015.[18]

Given new data showing that the costs of breaches in healthcare significantly exceed those of other sectors – healthcare breaches cost an average of $6.45 million, or 65% higher than the average cost in other sectors – the incentives for preventing the most commonly executed attacks are significant.[19]

WHERE SHOULD IDENTITY SOLUTIONS SIT IN AN ORGANIZATION?

Traditionally, most organizations have siloed IAM responsibilities in either Human Resources (HR) or Information Technology (IT) operations. There was a time when this made sense, given HR's role in onboarding and offboarding employees and the way IT ops fulfill day to day technology services. However, the threat model has shifted, as attackers race to exploit the opportunities presented by an approach to IAM that does not prioritize security and risk management.

Today, the CISO must take a leading role in IAM. This does not mean that the CISO alone must control every aspect of an organization's identity solutions – as we detail later in this paper, the most successful IAM projects involve leaders from a number of different components of their organization. However, it is imperative that CISOs acknowledge and embrace the fact that the factors that previously kept these components separate – and often kept identity out of the CISOs hands – have been eroded by shifts in technology and threat.

SIMPLE STEPS: WHERE & HOW TO START

While a full embrace of an identity-centric approach to cybersecurity will require significant work – much of which we will cover in future publications – there are three steps that H-ISAC members can take today to get started:

STEP 1

Commit to making identity a priority. It's a simple step, but one that's an essential starting point. To be clear, this is not just a commitment to invest in an upgrade of legacy IAM systems; rather, it's a decision to rethink the way your organization manages cyber risk today and commit to taking an identity-centric approach to it going forward.

STEP 2

Recognize that the CISO organization cannot do it alone. Begin partnering with the other stakeholders in your enterprise such as HR, CIO, Chief Customer Officer (CCO), Marketing, and anyone else likely to play a prominent role in IAM usage and implementation. There is a reason HR and/or the CIO previously owned identity, and the shift to a security-focused IAM approach does not mean those other stakeholders go away. The most successful IAM projects are driven through partnership.

Form a working group made up of these members that meets regularly. This working group can begin to develop a consensus on IAM issues and can begin to address what is changing across the enterprise with a focus on identity components and the scope of digital identities (visitors, prospects, customers, former customers, members, brokers, etc.) impacted today and in the future. Furthermore, this group will help ease the introduction of new projects, movements to the cloud, and the introduction of new infrastructure – by ensuring that identity is accounted for in each new product and project.

STEP 3

From a technology and architecture standpoint, conduct an IAM assessment that addresses the issues described in this paper. If you are not able to do an assessment yourself, contact the H-ISAC and they can assist, or put you in touch with other member companies who may be able to refer a provider. Additionally, consider how investments in an identity-centric approach to security can guard against the specific attack vectors outlined in this paper – while also enabling a more efficient business environment.

WHAT'S NEXT?

First in a Series

This paper represents the first of an H-ISAC series designed to introduce CISOs to an identity-centric approach to cybersecurity. By providing an explanation of key concepts, outlining a framework and best practices, investigating the various solutions and vendors, and highlighting the aspects of effective implementation, the H-ISAC intends to provide a holistic guide to assist CISOs in the health sector on how to best approach Identity and Access Management (IAM) and its role in managing cybersecurity risk.

More In-depth Analysis

Beyond this initial paper, members should expect H-ISAC subsequent releases to provide in-depth analysis and guidance on many of the issues introduced here.

Helping Organizations of All Sizes and Maturity Levels

The H-ISAC is committed to improving the entire healthcare cybersecurity ecosystem; this series will assist organizations of any size and of any cybersecurity maturity adapt their defense models to address the current threat landscape and become more secure.

References:

[1] https://www.reuters.com/article/us-verizon-yahoo/yahoo-strikes-117-5-million-data-breach-settlement-after-earlier-accord-rejected-idUSKCN1RL1H1

[2] https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/

[3] https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627

[4] https://www.cbc.ca/news/business/heartbleed-bug-rcmp-asked-revenue-canada-to-delay-news-of-sin-thefts-1.2609192

[5] https://www.csoonline.com/article/2466726/data-protection-heartbleed-to-blame-for-community-health-systems-breach.html

[6] https://www.reuters.com/article/us-sony-cybersecurity-costs/cyber-attack-could-cost-sony-studio-as-much-as-100-million-idUSKBN0JN2L020141209

[7] https://www.tripwire.com/state-of-security/security-data-protection/costs-3-major-email-security-breaches/

[8] https://www.cbsnews.com/news/irs-identity-theft-online-hackers-social-security-number-get-transcript/

[9] https://www.symantec.com/connect/blogs/opm-breach-costs-could-exceed-1-billion

[10] https://www.wired.com/story/dnc-lawsuit-reveals-key-details-2016-hack/

[11] https://www.reuters.com/article/us-uber-databreach/uber-settles-for-148-million-with-50-us-states-over-2016-data-breach-idUSKCN1M62AJ

[12] https://www.bankinfosecurity.com/equifaxs-data-breach-costs-hit-14-billion-a-12473 and https://abcnews.go.com/Technology/wireStory/equifax-pay-700m-data-breach-settlement-64481008

[13] See 2019 IBM Cost of a Data Breach Study https://www.ibm.com/security/data-breach and https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/, showing medical records selling for as high as $1000 per record.

[14] https://enterprise.verizon.com/resources/reports/dbir/2019/healthcare/

[15] https://www.ictsecuritymagazine.com/wp-content/uploads/2017-Data-Breach-Investigations-Report.pdf

[16] https://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf

[17] https://enterprise.verizon.com/resources/reports/dbir/2019/summary-of-findings/

[18] https://enterprise.verizon.com/resources/reports/dbir/2019/summary-of-findings/

[19] 2019 IBM Cost of a Data Breach Study https://www.ibm.com/security/data-breach