WHITE PAPER

# 5 Themes Driving Healthcare IT Company Investment

New innovations promise to increase efficiencies and reduce costs — but they also require a complementary focus on cybersecurity and protection.

# Executive summary

- The five themes that are driving healthcare IT (HCIT) company investment are: (1) managed services, hosting, and -aaS offerings; (2) funding, mergers and acquisitions (M&A), and the consolidation of technology companies; (3) interoperability, connectivity, and data aggregation; (4) artificial intelligence, machine learning, and analytics; and (5) developer toolkits.
- Healthcare is a prime target for cyberattacks, and HCIT companies are a common entry point. In fact, 60% of impactful healthcare cybersecurity attacks are caused by weaknesses among third-party vendors' security postures.
- Despite awareness among executives, cybersecurity is often overlooked, deprioritized, or identified too late by healthcare organizations. This hinders the value and satisfaction HCIT vendors can deliver without white-label or partner security solutions.
- The cybersecurity requirements are unique for each investment theme, including an assortment of government regulations and best practices to ensure protection.

The increased development of enterprise IT solutions and smart medical devices in healthcare and life sciences has provided incredible benefits, like improving patient access and experiences, lowering costs, and reducing operational inefficiencies.

The companies fueling and enabling this innovation cover a wide breadth of use cases, capabilities, and solutions — from medical devices and equipment to patient-facing software and data interoperability.

This surge in development has also been accentuated by Big Tech and the nontraditional healthcare companies that are expanding into the market. Recent examples include the emergence of Best Buy Health, the AWS purchase of One Medical, and Microsoft's acquisition of Nuance.

The healthcare companies that are driving innovation are investing in enhanced technical capabilities that streamline operations and increase the value delivered to customers. This places them in a strong position to take greater control of the market.

However, cybersecurity is often overlooked, deprioritized, or identified too late to develop adequate coverage and protection. Apps and infrastructure are underprotected and important initiatives often come in significantly over budget as a result.

This impacts HCIT companies across the healthcare ecosystem. One example is when HCIT company clients with insufficient cyberprotection receive additional, unexpected charges during implementation and deployment, which quickly lowers client satisfaction.

Customer organizations might also struggle with inadequate budgets, requiring the delay or cancellation of value-driving features. This reduces the value generated by the solution and lengthens the time to delivery. That's an important consideration for HCIT companies with a reputation to protect.

Thankfully, leaders are taking notice. As of July 2020, 69% of medical technology executives said cyber readiness will be their highest priority over the next five years. However, their collective actions don't reflect that priority yet.

Prioritizing cybersecurity requirements alongside technical investment decisions is the best way — the only way — to avoid risk and protect products, customers, and patients.

You can save your organization from the consequences and economic impacts of cyberattacks (Table 1).

| Consequences of Cyberattacks | Economic Impact |
|---|---|
| Data breaches | • Damaged reputation, loss of trust |
| Ransomware | • Ransom cost<br>• Lost revenue from operational downtime<br>• Patient lives or outcomes at risk due to unavailable data or critical care delivery tools (e.g., robotic surgical devices) |
| Unauthorized access | • Lost data or works in progress<br>• Costs and lost revenue from operational standstill |
| Rebuilding systems after the attack | • Costs of rebuilding<br>• Lost revenue from the subsequent operational standstill |

*Table 1: The consequences and costs of cyberattacks*

## The five themes in HCIT investments

Let's take a closer look at the five themes in HCIT investments and the best practices companies should take to ensure protection against cybersecurity threats.

### 1. Managed services, hosting, and -aaS offerings

Technology companies are increasingly moving away from traditional business models. Vendors (and buyers) are no longer reliant on perpetual, on-premises licenses; they now prefer cloud-hosted deployments.

Healthcare is also progressing toward managed service offerings, in which the HCIT product is configured and deployed in the cloud, and the vendor organization maintains the management. Some HCIT vendors are even moving to full-service offerings, in which the buyer organization only needs to deploy minimal resources to get the full benefits of the offering.

Managed services, hosting, and -aaS offerings for HCIT companies can provide:

- Increased efficiency and scalability from the solution's cloud deployment
- Recurring, long-term, and predictable revenue streams
- The efficiency and affordability of cloud-based customer service
- Significantly faster time to value compared with on-premises solutions

## 2. Funding, M&A, and the consolidation of tech companies

Although investment has slowed slightly from the breakneck pace of 2021, consolidation and inorganic growth among HCIT companies still drive progress in this part of the healthcare ecosystem.

From venture-backed start-ups to growth companies backed by private equity to publicly traded behemoths, inorganic growth is projected to remain a significant trend among HCIT organizations, particularly as a segment entry point for Big Tech. Recent examples include Oracle and Cerner, Optum and Change Healthcare, and Walgreens-VillageMD and CareCentrix.

Funding, M&A, and consolidation for HCIT companies can provide:

- Accelerated growth by expanding into new market segments and buyers, and increasing product capabilities through mature companies
- The ability to meet buyers' desire for vendor consolidation by offering a more robust product suite
- Economies of scale through operational efficiencies
- Incentive alignment through vertical integration across the value chain

## 3. Interoperability, connectivity, and data aggregation

Healthcare data has historically been siloed in various systems across the patient care journey and healthcare delivery value chain. With the increased adoption of third-party solutions, information is more fragmented than ever. The differences in datasets and models prove to be a significant challenge to HCIT companies' efforts to achieve interoperability during the implementation and deployment processes.

However, the power of healthcare data is enormous for nearly every stakeholder and workflow. The need to connect IT and medical device systems to data sources in an interoperable, standardized way is essential for the future of healthcare technology.

The U.S. government recognizes this and is increasingly mandating that vendors and organizations facilitate the secure sharing of data. These mandates are a driving force in buyers' decision-making, requiring them to choose solutions that enable regulatory compliance and optimize the data sharing across user groups and workflows.

Interoperability, connectivity, and data aggregation for HCIT companies can provide:

- Better service for patients, providers, and other relevant stakeholders through the complete set of information on a patient or workflow
- Improved clinical decision-making and accelerated speed to care through the availability of relevant data
- Stronger tech solutions and a better end-user experience through the availability of accurate, complete, and real-time patient data

## 4. Artificial intelligence, machine learning, and analytics

It’s becoming ever more prevalent for both buyers and vendors to empower computers to develop intelligence that can autonomously perform human tasks through artificial intelligence. This allows organizations to visualize and analyze data that derives powerful insights, which enables better decision-making for the end user.

These technologies also bring additional cybersecurity challenges that require attention and consideration. For example, data collected from remote patient-monitoring devices can inform artificial intelligence for individual patients and the broader population. But without bolstering the network edge and restricting the extent of a breach with a microsegmentation solution, the organization’s entire network is at risk.

Artificial intelligence, machine learning, and analytics for HCIT companies can provide:

- Analyses of large datasets to understand the implications, benefits, and success rates of products on the market
- The ability to make better business decisions to increase efficiencies, decrease costs, and better target the pain points of buyers and end users
- Faster and more accurate information processing to improve efficiency and quality in core product use cases and workflows
- Improved patient outcomes and access through predictive models, increased patient satisfaction scores, and better reimbursement rates for value-based care provider organizations

## 5. Developer toolkits

Software development kits (SDKs) and other similar products or services make the ideation, scoping, development, testing, and deployment of new HCIT offerings faster and more efficient.

Although convenient, SDKs can increase the number of cybersecurity vulnerabilities because of the inherent unknowns when another company's code is used for the solution. Once threat actors identify a vulnerability, it can be exploited in every active solution and instance that uses that SDK.

Developer toolkits for HCIT companies can provide:

- Faster development cycles through enhanced transparency, better project and product management, and improved cross-team and cross-functional communication
- The ability to build on existing tools and functionality instead of starting from scratch
- Decreased development costs from low-code or no-code tools that require fewer technical resources to achieve the end result
- The ability to leverage existing toolkits and expertise to facilitate the use and adoption of best practices for healthcare

# The need-to-know on cybersecurity

Cybersecurity-related regulations affecting HCIT investment include The Health Insurance Portability and Accountability Act of 1996 (HIPAA), the 21st Century Cures Act, and the Quality System Regulation (QSR) (Table 2).

| Relevant Regulations | Area(s) of Concentration |
|---|---|
| **HIPAA** — Protects personally identifiable information and protected health information | • Managed services, hosting, and -aaS offerings<br>• Funding, M&A, and the consolidation of technology companies<br>• Interoperability, connectivity, and data aggregation<br>• Artificial intelligence, machine learning, and analytics<br>• Developer toolkits |
| **21st Century Cures Act** — Enables patients to have access to their own data | • Funding, M&A, and the consolidation of technology companies<br>• Interoperability, connectivity, and data aggregation |
| **QSR** — Regulations for medical devices and wearables | • Managed services, hosting, and -aaS offerings |

*Table 2: The cybersecurity-related regulations affecting HCIT investment*

You can protect your organization with the cybersecurity capabilities that are most important to the five HCIT investment themes (Table 3).

| How to Ensure Protection | Area(s) of Concentration |
|---|---|
| **Secure your infrastructure**<br>• Harden the outside of your infrastructure with a DDoS mitigation tool<br>• Bolster the inside of your infrastructure with a microsegmentation solution | • Managed services, hosting, and -aaS offerings<br>• Funding, M&A, and the consolidation of technology companies<br>• Interoperability, connectivity, and data aggregation |
| **Secure your access**<br>• Zero Trust Network Access<br>  • Multi-factor authentication to avoid account takeovers<br>  • Secure web gateway | • Managed services, hosting, and -aaS offerings<br>• Funding, M&A, and the consolidation of technology companies<br>• Artificial intelligence, machine learning, and analytics<br>• Developer toolkits |
| **Secure your applications and APIs**<br>• Secure web applications and APIs to ensure data and analytics outcome integrity | • Managed services, hosting, and -aaS offerings<br>• Funding, M&A, and the consolidation of technology companies<br>• Interoperability, connectivity, and data aggregation<br>• Artificial intelligence, machine learning, and analytics<br>• Developer toolkits |
| **Have the resources and expertise to correctly set up and manage cybersecurity solutions** | • Managed services, hosting, and -aaS offerings<br>• Funding, M&A, and the consolidation of technology companies<br>• Interoperability, connectivity, and data aggregation<br>• Artificial intelligence, machine learning, and analytics<br>• Developer toolkits |

*Table 3: The most important capabilities for protecting against cyberattacks*

## Conclusion

All the dynamic innovation happening in the HCIT market introduces cybersecurity challenges that must be addressed proactively. This is especially true for larger, multi-industry organizations that are working to navigate healthcare pain points and regulations for the first time.

As an industry, healthcare is a prime target for cyberattacks, and HCIT companies are a common entry point. In fact, 60% of successful healthcare cybersecurity attacks are initiated through third-party vendors.

Make sure you are working with a trusted leader in the healthcare cybersecurity space. Having a partner like Akamai, with the right products, expertise, and resources, ensures that you are adequately protected against malicious actors amid your technology investments.

**Contact Akamai for a deeper dive into which solutions would benefit your organization the most.**

Akamai powers and protects life online. Leading companies worldwide choose Akamai to build, deliver, and secure their digital experiences — helping billions of people live, work, and play every day. Akamai Connected Cloud, a massively distributed edge and cloud platform, puts apps and experiences closer to users and keeps threats farther away.Learn more about Akamai's security, compute, and delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on Twitter and LinkedIn. Published 03/23.