TREND 4:

SECURE US TO SECURE ME

Enterprises are not victims, they're vectors

The need for collaboration is as great in healthcare as in any other industry.

Healthcare organizations enjoy the benefits of collaborating with the ecosystem—providers, payers, device companies, equipment manufacturers and more—but those connections increase risk. Through collaboration, businesses are extending, and absorbing, the risk and vulnerabilities of their ecosystem partners. Yet most businesses still look at cybersecurity as strictly an individual effort.

It's an especially tough spot for healthcare organizations because unlike in other industries, they sometimes don't have a choice about with whom they collaborate. It's a mandate.

This heightened level of exposure is good news for the "bad guys" who view ecosystems as an ever-widening attack surface. Healthcare businesses must, in response, evolve their approach and stand up a stronger security posture that factors in ecosystem partners. New models and policies must ensure that the partners and third parties joining the ecosystem adhere to the same standard of security—or higher—that they set for themselves.

It is not easy. As such, 77% of healthcare executives agree that protecting their organization in an ecosystem relies on security practices that they have limited ability to control. Fortifying the security posture calls for factoring in growing ecosystem dependencies. While healthcare organizations already collaborate to deliver best-in-class products, services and experiences, it's time for security to join that effort as well.

EXAMINING RISK

The first step to securing any enterprise is understanding the potential threats on the horizon and the subsequent risk those threats pose. It is becoming increasingly challenging to identify where threats lie, but meanwhile **attacks are increasing in scope.**[1] In a **February 2018 survey**, payers said that cyber attacks targeting payers were up 89% in the previous year,[2] and 65% of providers said cyber attacks remain a "black box" in terms of when and how they will impact the organization.

Even apps that may seem benign or helpful might present dangers. Consider how **Strava,** a fitness app, had to suspend services after it was discovered that **the app's anonymized activity map was inadvertently uncovering classified US military sites** as soldiers tracked their workouts.[3] The data did not present significant risk to Strava or any privacy risk to individuals, as it was aggregated and not personally identifying. But it was this very aggregation, coupled with free access to the information, that generated substantial risk for a subset of the company's customer base—and, in fact, for a large group of non-Strava users as well.

It's immensely challenging for both payers and providers to understand third-party risk. For instance, devices are present in the care environment, and **these can present potentially life-threatening risks**.[4] In a worst-case scenario, a device or piece of equipment could be infiltrated to hurt a patient. Imagine the dialysis pump that delivers a lethal dose. **Devices can also serve as an entry point to harm the provider's entire system.**[5]

Risk resides in data being used on an external device inside a hospital. For instance, healthcare employees often use their own personal devices to share information. How can the enterprise better protect the hospital or health plan from security risks related to those devices?

Many questions remain and the only way to solve them is to work together to find the answers.

SECURITY FOR ALL

Health information is particularly sensitive, due to considerations such as data from patients who do not want to disclose health issues to their employers. Privacy and security are coupled in healthcare, presenting even greater complexity.

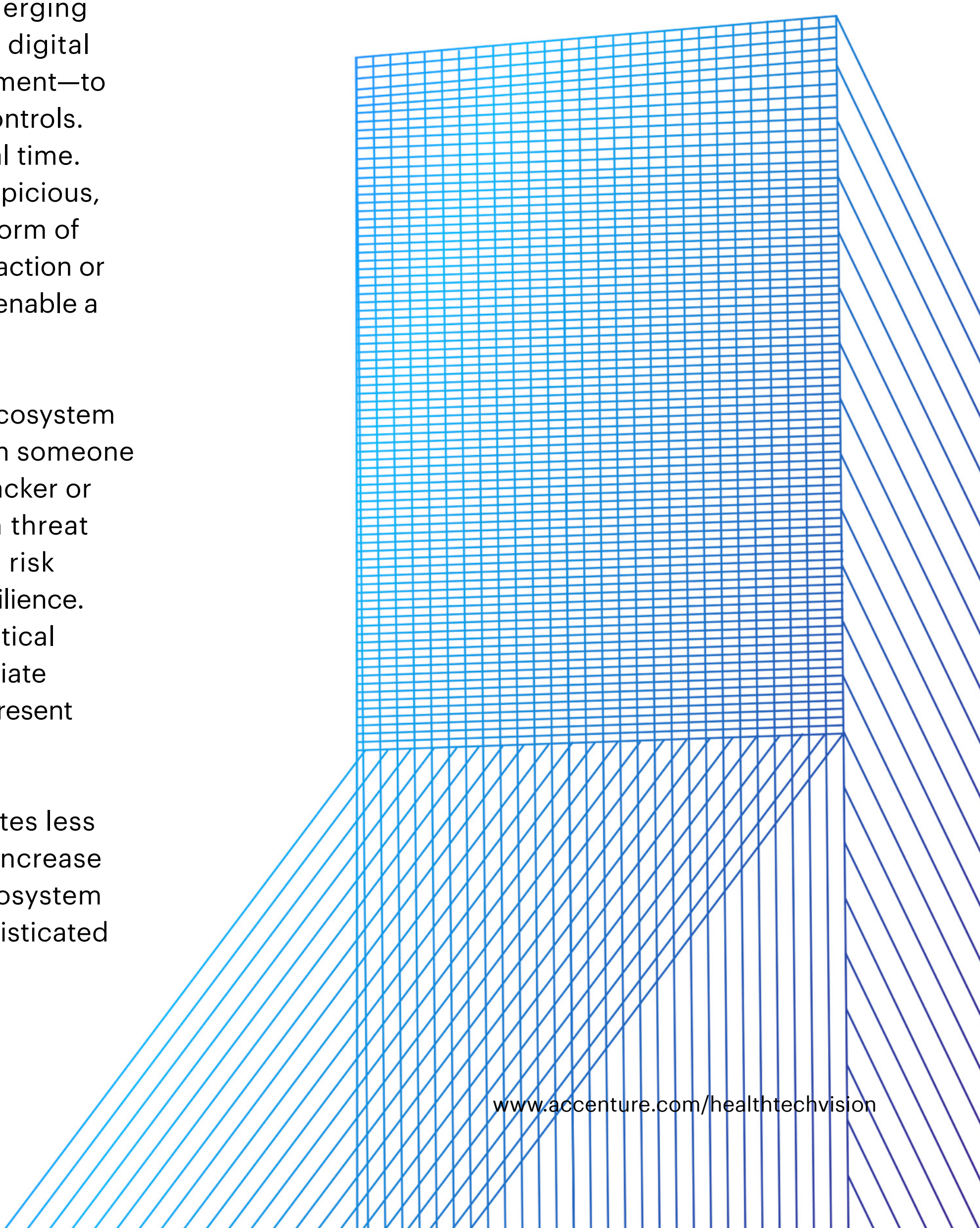
Ecosystem participants bring unique strengths and talents and can work together to improve security. One way to do so is to join forces to conduct a mock attack. The team would create certain issues (e.g. a breach featured on the news, an asset that unexpectedly became unavailable) and test the level of preparedness. The organization's executive, legal, human resources and communications teams would be tasked with reacting to these scenarios.

Such exercises illustrate the fact that threats are on the move. Therefore, the industry can no longer have static models for controls. Risk modeling must be more dynamic, at an interaction level. Healthcare organizations can work with established and emerging players—such as those working in digital identity or privileged user management—to create real-time, decision-based controls. These controls thwart threats in real time. For instance, if an interaction is suspicious, the system would require another form of validation and either block the interaction or require a call from the help desk to enable a different avenue of access.

Threat modeling across an entire ecosystem lets organizations put themselves in someone else's shoes, whether that is an attacker or a partner. Doing so improves both threat intelligence and understanding of risk exposure—and strengthens their resilience. It enables companies to identify critical dependencies that demand immediate hardening, or vulnerabilities that represent potential damage to a partner.

This dynamic type of security creates less friction for consumers, and it can increase trust as patients, members and ecosystem partners know there are more sophisticated security practices at play.

As vulnerabilities increase, so does the burden on already overworked security professionals. Healthcare organizations can stem potential mistakes and oversights by embracing DevSecOps—integrating security teams into DevOps teams to allow for continuous improvements to security. In this way, enterprises can spread responsibility for and ownership of security throughout their organization, giving security teams the agility to address the biggest challenges. By being more strategic with how they position security internally, healthcare organizations can make it a business enabler, rather than a catch-all.



92%

of healthcare executives agree that to be truly resilient, organizations must rethink their approach to security in a way that defends not just themselves, but their ecosystems.

87%

of healthcare executives agree that security in their organization is evolving from a siloed function to a critical component of their strategy, reputation and relationships.

NEXT-GENERATION IDENTITY ACCESS MANAGEMENT

To help large organizations struggling to manage and secure the fluid nature of user privileges, Accenture Security created **Zoran, an identity management capability powered by artificial intelligence**. The solution aggregates data from multiple systems and sources to generate a confidence score for each user—low scores indicate potentially risky access and high scores can be considered for automated approvals. The system can also predict and recommend access needs for new joiners in a company, saving time, money and effort in the onboarding process. By transforming the way user access privileges are managed, monitored and controlled, healthcare organizations can reduce the risk and costs associated with the over-provisioning of accounts tied to a user's identity.

"We see enormous potential to transform our current identity access model from a static interface to a dynamic, intelligent and scalable resource that can increase efficiency and reduce costs," said Kurt Lieber, chief information security officer of Aetna. "This type of transformation gives us the ability to make better decisions faster, so the right people get access to the right business resources at the right time."

Related

Accenture 2018 State of Cyber Resilience for the Healthcare Industry

The Cost of Cybercrime to the Healthcare Industry

Spending Smart to Defend Against Healthcare Cybercrime

Sources

[1] U.S. Department of Health and Human Services Office for Civil Rights Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information; https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[2] "Becoming Cyber Resilient in Healthcare;" Accenture, January 18, 2019; https://www.accenture.com/us-en/insights/health/improving-cybersecurity-healthcare

[3] "How Strava's 'Anonymized' Fitness Tracking Data Spilled Government Secrets;" Zdnet, January 29, 2018 https://www.zdnet.com/article/strava-anonymized-fitness-tracking-data-government-opsec/

[4] "When Medical Devices Get Hacked, Hospitals Often Don't Know It;" Healthcare IT News, May 11, 2018; https://www.healthcareitnews.com/news/when-medical-devices-get-hacked-hospitals-often-dont-know-it

[5] "Hacked Medical Devices Could Wreak Havoc on Health Systems;" Modern Healthcare, January 20, 2018; https://www.modernhealthcare.com/article/20180120/NEWS/180129999/hacked-medical-devices-could-wreak-havoc-on-health-systems

For more information:

KAVEH SAFAVI, M.D., J.D.
kaveh.t.safavi@accenture.com

BRIAN KALIS
brian.p.kalis@accenture.com

ANDREW THOMPSON
andrew.j.thompson@accenture.com

Follow us

@AccentureHealth

/AccentureHealth

About Accenture 2019 Technology Vision Survey

Accenture conducted a global survey of thousands of business and IT executives to understand their perspectives on the impact of technology on their organizations, and to identify their priority technology investments over the next few years. More than 6,600 executives from 27 countries responded to the survey, including 221 US and Canadian healthcare executives. The survey was fielded from October 2018 through December 2018.

Disclaimer
In some cases, some of the references to companies or products herein may include companies or products which Accenture supports or provides services to. Accenture is in no way promoting or intending to market any one particular company, solution or product or otherwise offer or market a medical device or clinical solution or services.

About Accenture Insight Driven Health

Insight driven health is the foundation of more effective, efficient and affordable healthcare. That's why the world's leading healthcare providers and health plans choose Accenture for a wide range of insight driven health services that help them use knowledge in new ways—from the back office to the doctor's office. Our committed professionals combine real-world experience, business and clinical insights and innovative technologies to deliver the power of insight driven health.

For more information, visit:
www.accenture.com/insightdrivenhealth

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions — underpinned by the world's largest delivery network — Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With 477,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives.

Visit us at **www.accenture.com**