# IMPLEMENTING THREAT-BASED CYBERSECURITY TO SECURE PATIENT CARE INNOVATION

BDO

Technology has brought healthcare to consumers' fingertips, putting them at the nucleus of care and blurring the definition of a healthcare organization.

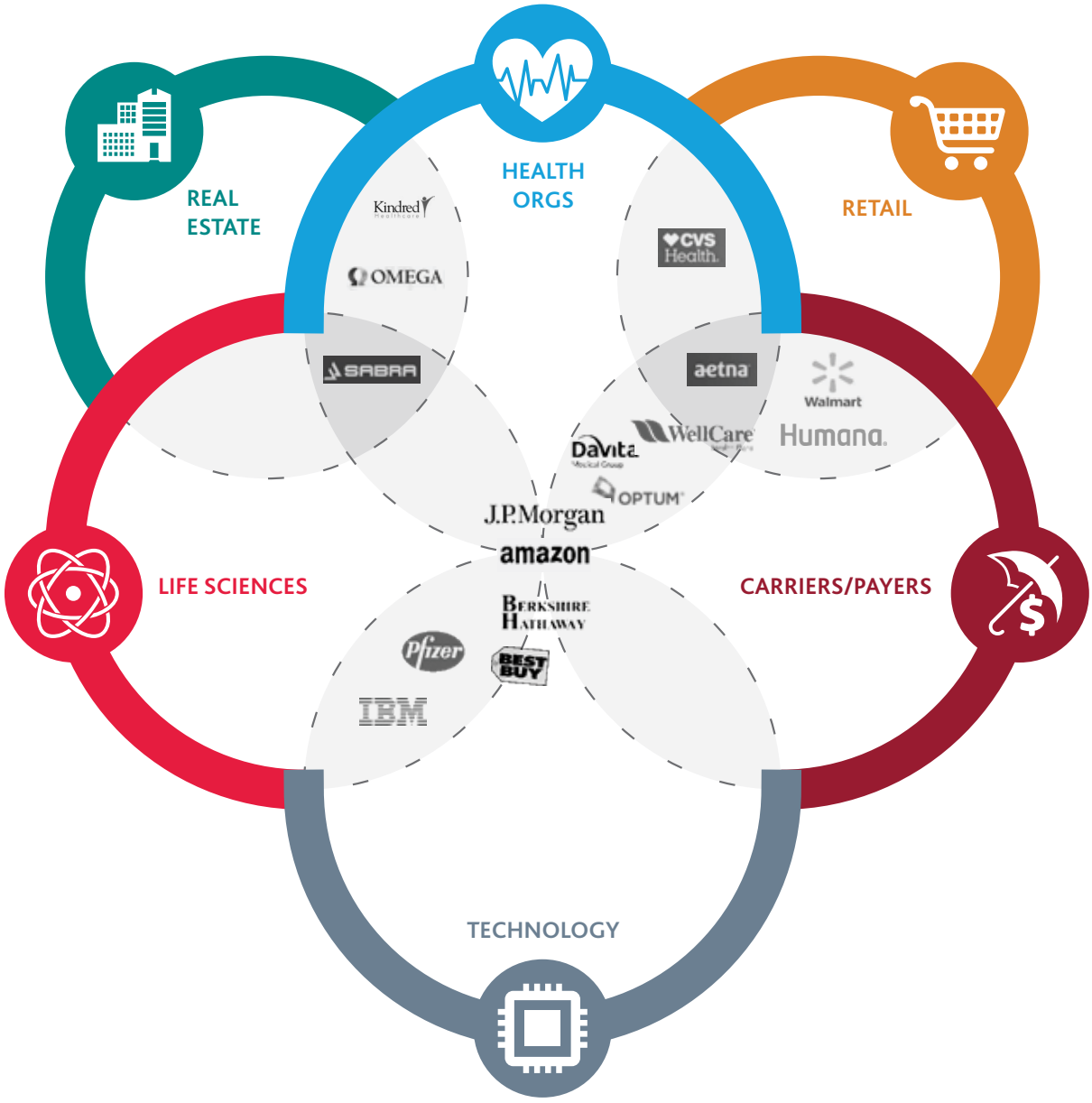
Traditional technology entities are building healthcare apps, wearables and other connected devices, and consumers are using them to track their health progress and feed data back to their provider, payer or both. Retailers are partnering with pharmacies, so both can gain access to each other's data and reach a greater number of consumers. Insurers are partnering with pharmaceutical manufacturers to leverage patient data to improve outcomes and lower health costs.

But perhaps nothing says the healthcare company of the future has arrived as best as the innovative partnership between Amazon, JPMorgan and Berkshire Hathaway.

Data-sharing between consumer health organizations is of course net positive. Capitalizing on data is the first step to achieving precision medicine and creating shared value across the health ecosystem. But cyber risks are also growing as data sharing increases.

If organizations in the business of consumer health are going to sustainably innovate around patient care, they must be able to safely store and analyze patient data—the most valuable resource to the consumer, to the business of health and, we believe, to the security of a nation.

Threat-based cybersecurity will be their lifeline.




Read more ▶

## THREAT-BASED CYBERSECURITY: A CONDENSED ROADMAP

Based on intent, threat-based cybersecurity is a forward-looking, predictive approach. Instead of (or in addition to) focusing solely on protecting critical data assets or following the basic script of a generic cyber program, threat-based cybersecurity concentrates investments in **the most likely risks and attack vectors based on your company's unique threat profile**.

How do healthcare organizations develop and maintain a comprehensive cyber threat profile?

The first step is to assess and take ownership of your organizational DNA: the data assets and other intellectual property that make you unique—or a potential target. Owning your organizational DNA starts with information governance: identifying, managing, accurately categorizing, protecting and optimizing organizational data from inception to final disposition.

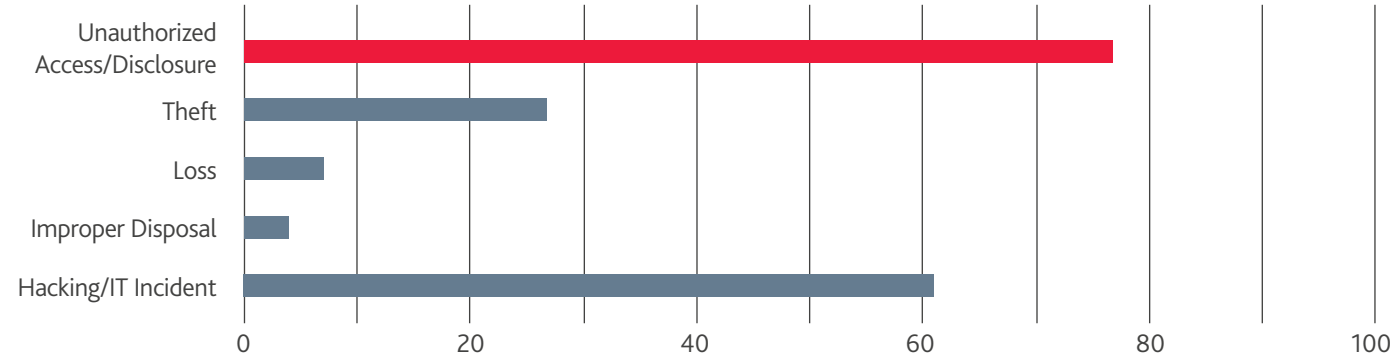
But, keep in mind that the data assets you value most may not be the prime target for a would-be hacker. Your data on performance outcomes, for example, is far harder to monetize on the dark web than your patient database.

The next step is to factor in the threat environment to understand current exploits and the most targeted vulnerabilities.

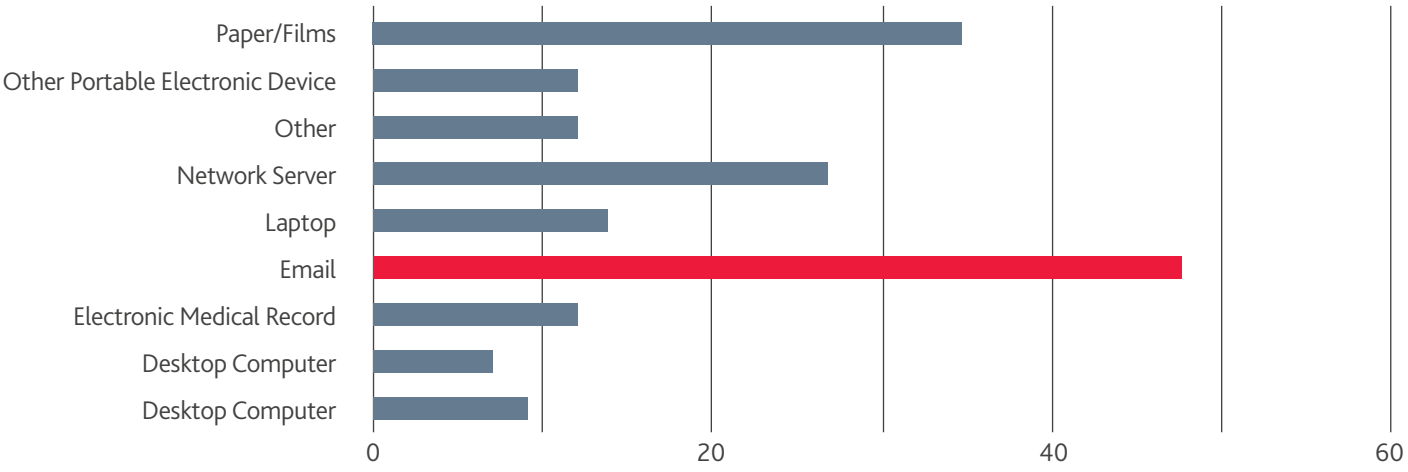
As of July 12, so far this year the U.S. alone has seen 176 reported large-scale data breaches (those impacting 500 or more individuals), according to the **U.S. Department of Health & Human Services**. That number equates to 3.2 million patients impacted and spans 40 states.

But more telling are the **breach types** and **locations of breached information**. The biggest threats in 2018 have been unauthorized access/disclosure (77) and email (48), respectively.

**TYPE OF BREACH**




**LOCATION OF BREACHED INFORMATION**




Read more ▶

What this tells us is that, to effectively detect and respond to risks, healthcare organizations need to:

**Bolster their access controls –** technical policies and procedures to ensure only authorized employees have access to protected health information (PHI) via Electronic Health Records (EHR), and personal identifiable information (PII)—and be more stringent about who they grant access.

**Implement stronger audit controls –** to track and identify internal and external access to and exploration of information systems that contain PHI and PII.

**Strengthen intrusion detection systems (IDS) –** to more accurately monitor traffic moving throughout their email, network, and information system endpoints to identify suspicious activity and clear threats in real time.

**Make top-down personnel education a priority for everyone (from the Board of Directors, to the C-Suite, managers, and employees) –** to ensure all individuals with access to an organization's networks, medical devices and data understand their roles and responsibilities in defending against cyber threats.

**Create an internal and external crisis communications plan –** to align with existing enterprise risk management frameworks (i.e., HIPAA, HITRUST, NIST, etc.).

**Implement cyber insurance claims preparedness and adequate coverage –** to identify and quantify incurred event response costs for inclusion in an insurance claim.

**Create an incident response plan –** to include the participation of organization leadership and key personnel from all technology, business, administration and clinical functions.

**Develop and test a Business Continuity Plan (BCP) –** in order to have real information resilience it is vital to have an effective information back-up capability which is able to quickly replace any data loss.

Capitalizing on data is one of the first steps to innovating patient care—and is crucial to surviving in today's blurry healthcare ecosystem. But to do so sustainably, in a way that protects patient privacy and data security, will require a threat-based approach to cybersecurity.

And achieving threat-based cybersecurity is a journey spanning the entire corporate lifecycle.

Learn more about how we can help you throughout your unique lifecycle.

## CONTACT

**GREGORY GARRETT**
Head of U.S. and
International Cybersecurity
703-770-1019 / ggarrett@bdo.com

**ANDREW SILBERSTEIN**
Director, Cybersecurity
Advisory Services
703-770-0537 / asilberstein@bdo.com



Read more ▶