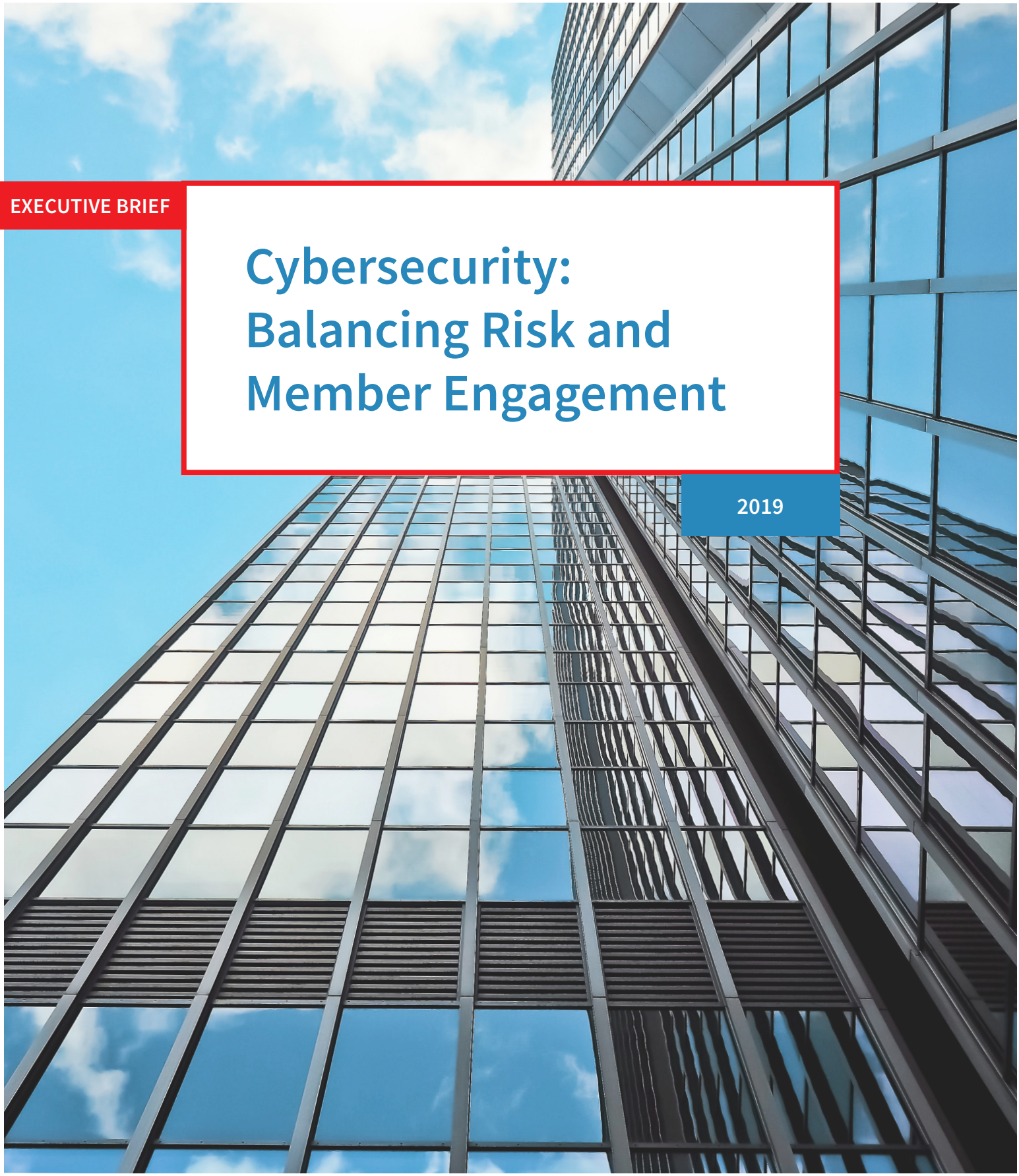
mcol

LexisNexis® RISK SOLUTIONS | Health Care



EXECUTIVE BRIEF

Cybersecurity: Balancing Risk and Member Engagement

2019

The rise in digital health initiatives present more vulnerabilities than ever before in security of patient data. As a result, healthcare organizations are experiencing a record number of data breaches and suffering millions of dollars in fines, settlements and operational losses. Experts from LexisNexis® Risk Solutions Health Care met with an audience of healthcare stakeholders to discuss ways to reduce the risk of a data breach, explain the necessary steps to validate and verify member information, and identify the ingredients for a strong multi-factor authentication strategy.

Erin Benson, Director Market Planning, LexisNexis Risk Solutions Health Care, tells us "With a growing number of data breaches, the need for cybersecurity and physical security keeps CIOs up at night. At the same time, value-based care and the rise of consumerism are driving the need to provide members with a quality experience without introducing a lot of friction into the process."

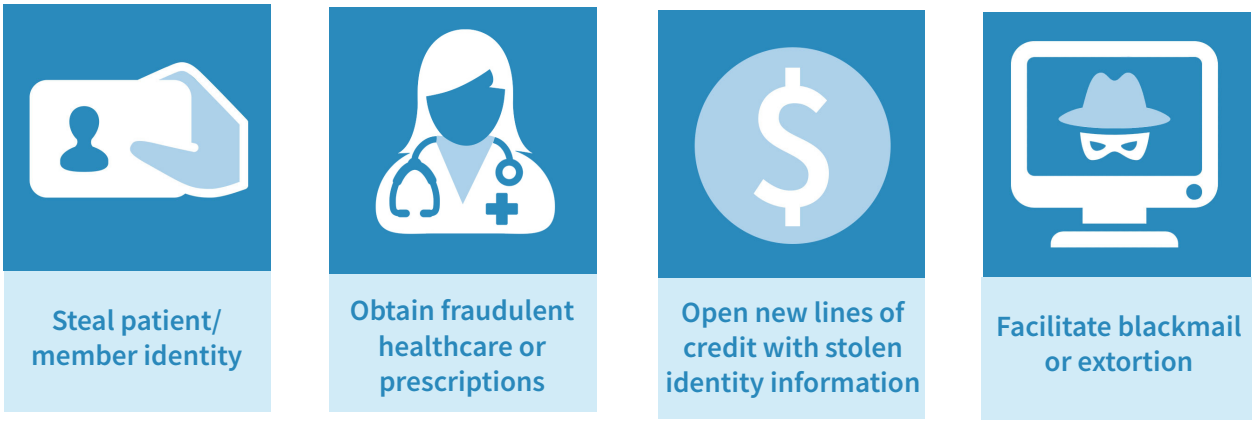
"These two needs are fundamentally at odds. Cybersecurity calls for more secure access gates, while member engagement calls for more ease of use of online portals and other healthcare services."

This webinar features a discussion on market trends in digital security and member engagement, the role of a universal member identifier, layers of defense required for optimal data security and how to balance these efforts.

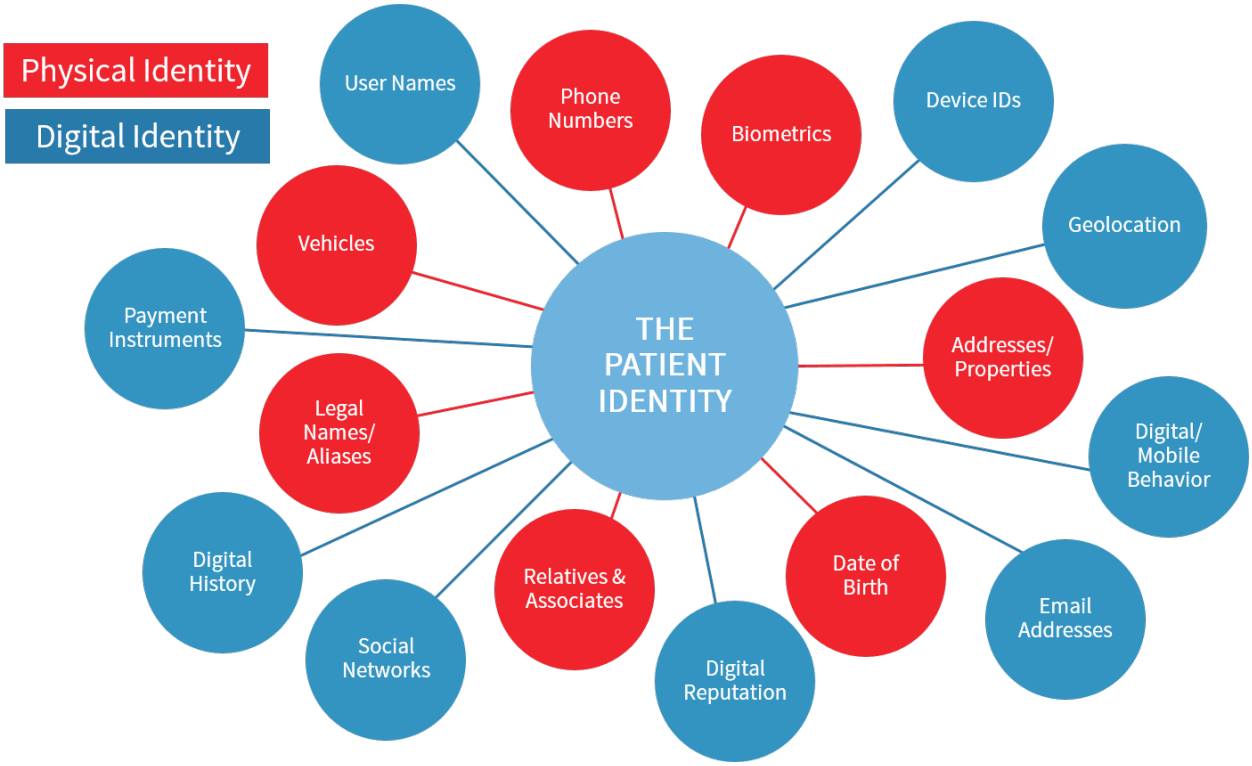
Through the engagement of a member portal, members can:

- View and get answers to coverage questions
- Track claims and account activity
- Locate doctors and services
- Find health advice
- Manage member profile
- Pay bills

Fraudsters targeting healthcare firms to:

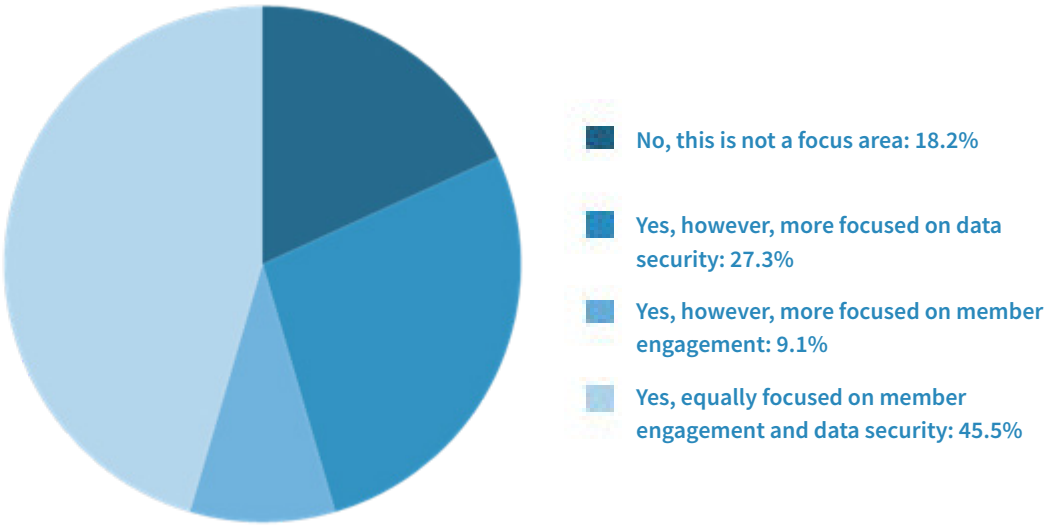


Courtney Timmons, Market Planning Specialist, LexisNexis Risk Solutions Health Care, tells us "having the ability to assess and link physical and digital identity datapoints, such as a person's digital behavior to vehicles, phone numbers, addresses, dates of birth, relatives and associates, is key in protecting member populations."



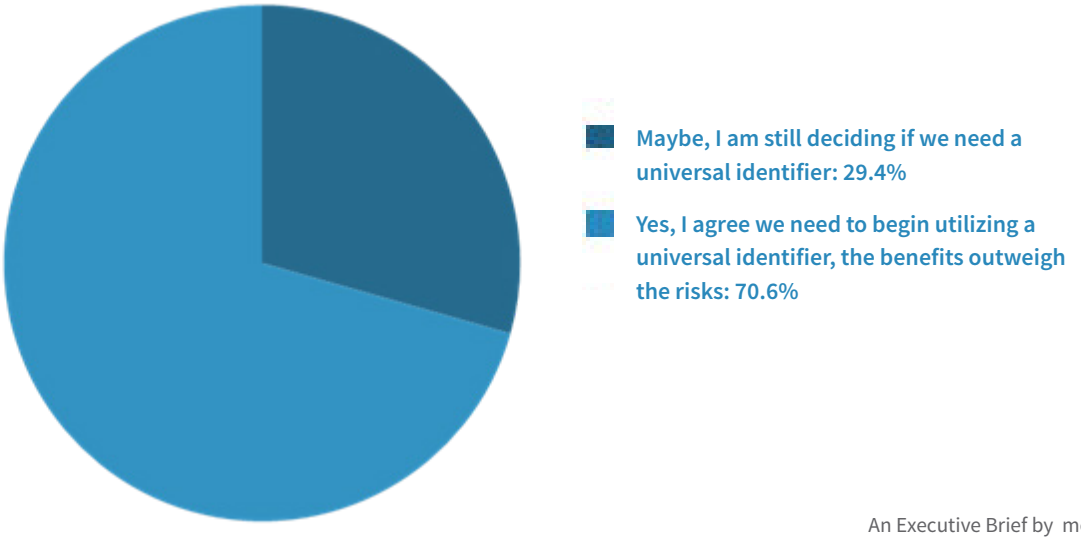
The audience weighed in on their efforts to achieve balance with these opposing initiatives within their company. When asked "Is your organization addressing the challenge of balancing member engagement and data security?" almost 75% indicated focus related to data security:

Is your organization addressing the challenge of balancing member engagement and data security?



Since the advent of the Health Insurance Portability and Accountability Act (HIPAA) almost two decades ago, there's been much discussion about adoption of a unique health identifier for every individual. It's clear that with advances in digital technology, it's more important than ever to move towards a universal identifier, and the audience agrees.

When asked, "Is a universal identifier important to the future of healthcare?" close to three quarters agree that we need to begin utilizing a universal identifier:

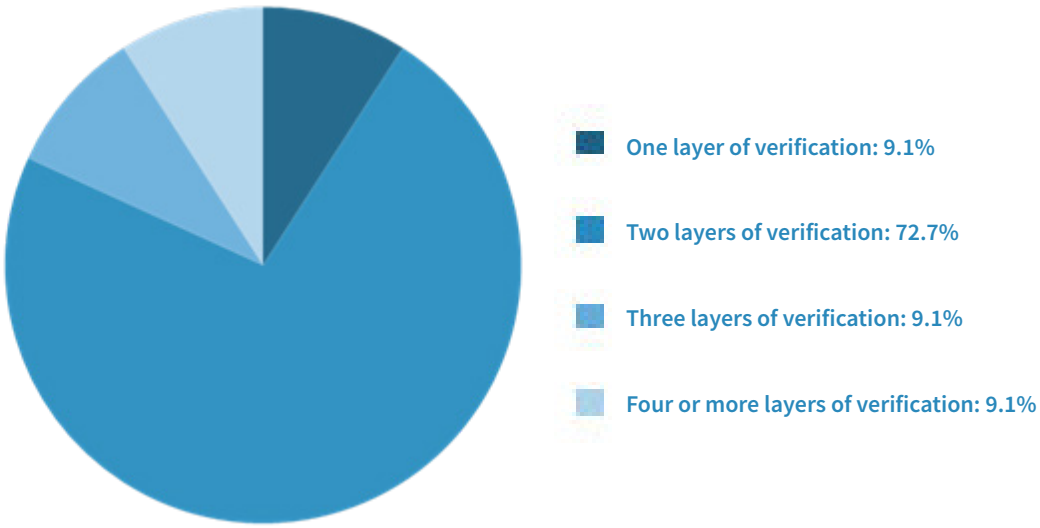


It is imperative to build the right level of verification and authentication across workflows so that the right members get through with little to no friction, and the fraudsters are kept out, hitting several security blocks due to the detection of synthetic or manufactured identity information, or their lack of proof that they are who they say.

Identity Verification Layers

How you act	How you compare to others	Something you are	What others know about you	Something you have	Something you know
Contextual Based	Analytics Based	Biometric Based	Contributory Based	Possession Based	Knowledge Based

Most healthcare organizations are investing in new infrastructures to continually analyze existing workflows and highlight access methods and gaps where potential fraud may occur. The audience was polled on how many layers of verification their organization is using:



Cybersecurity vulnerabilities and threats in healthcare are very real. According to a Report on Improving Cybersecurity in the Health Care Industry, published by the Health Care Industry Cybersecurity Task Force, the Task Force identified six imperatives that must be achieved to increase security within the healthcare industry:

1	Define and streamline leadership, governance, and expectations for healthcare industry cybersecurity.
2	Increase the security and resilience of medical devices and health IT.
3	Develop the healthcare workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities.
4	Increase healthcare industry readiness through improved cybersecurity awareness and education.
5	Identify mechanisms to protect R&D efforts and intellectual property from attacks or exposure.
6	Improve information sharing of industry threats, risks, and mitigations.

To watch the full one hour webinar, visit: https://risk.lexisnexis.com/insights-resources/webinar/cybersecurity-and-member-engagement

For more information, call 866.396.7703 or visit risk.lexisnexis.com/healthcare

LexisNexis® RISK SOLUTIONS

About LexisNexis Risk Solutions

LexisNexis Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX Group (LSE: REL/NYSE: RELX), a global provider of information and analytics for professional and business customers across industries. RELX is a FTSE 100 company and is based in London. For more information, please visit www.risk.lexisnexis.com, and www.relx.com.

Our healthcare solutions combine proprietary analytics, science and technology with the industry's leading sources of provider, member, claims and public records information to improve cost savings, health outcomes, data quality, compliance and exposure to fraud, waste and abuse.