Executive Perspectives on Top Risks – Key Issues Being Discussed in the Boardroom and C-Suite

Research conducted by Protiviti and North Carolina State University’s ERM Initiative


These and a host of other significant risk drivers are all contributing to the risk dialogue happening today in boardrooms and executive suites.

Expectations of key stakeholders regarding the need for greater transparency about the nature and magnitude of risks undertaken in executing an organization’s corporate strategy continue to be high. Pressures from boards, volatile markets, intensifying competition, demanding regulatory requirements, changing workplace dynamics, shifting customer preferences, uncertainty regarding catastrophic events and other dynamic forces are leading to increasing calls for management to design and implement effective risk management capabilities and response mechanisms to identify, assess and manage the organization’s key risk exposures, with the intent of reducing them to an acceptable level.
In this seventh annual survey, Protiviti and North Carolina State University’s ERM Initiative report on the top risks on the minds of global boards of directors and executives. Our respondent group, which includes 825 board members and C-suite executives from around the world, provided their perspectives about the potential impact over the next 12 months of 30 risk issues across these three dimensions:

- **Macroeconomic risks** likely to affect their organization’s growth opportunities
- **Strategic risks** the organization faces that may affect the validity of its strategy for pursuing growth opportunities
- **Operational risks** that might affect key operations of the organization in executing its strategy

**Commentary – Healthcare Industry Group**

**Regulatory changes and regulatory scrutiny**

The healthcare landscape continues to evolve, with regulatory changes and scrutiny on the rise. This trend continues due to pressure to reduce regulation and control regulatory costs. Additionally, there has been an increase in public engagement advocating for more transparency, increased public notice and due process in rulemaking. The cost of staying on top of regulatory changes has increased, in part, by imposing significant fines and take-backs for fraud, waste and abuse violations; increased head count for coverage; and increased NDO insurance costs due to individual liability becoming more commonplace. In addition, the rise of professional whistleblowers has proven to be a lucrative occupation. An upswing in provider audits will occur, namely with the new targeted, probe-and-educate method to become the most prevalent audit method used by Medicare Administrative Contractors. The collaboration between various government agencies (e.g., Office of Inspector General (OIG), Centers for Medicare and Medicaid Services (CMS), Office of Civil Rights (OCR), and Department of Justice (DOJ)) has exposed the largest healthcare fraud takedown in history – sending a strong message that fraud and abuse will not be tolerated.¹

The Affordable Care Act remains on uncertain ground as tax reform promises to end the individual mandate, which will mean fewer Americans with health insurance, and likely fewer doctor visits and hospital stays. Additionally, this will result in a decrease in the amount of drugs and medical devices sold. Constraints to access to healthcare will be eased with the growth of telemedicine. The opioid crisis will continue to take center stage, resulting in an increase in mental health and treatment facilities. Additionally, enforcement agencies will increase focus on physician prescribing patterns in the coming year, as elevated scrutiny of the 340B Drug Pricing Program is being felt across the industry. Specific examples include increased Human Resources and Services Administration (HRSA) audits and the need for annual independent audits of contract pharmacy

arrangements. Ultimately, implementing robust and effective compliance programs will be key to understanding and mitigating risk and managing the complex regulatory landscape.

Key compliance areas of focus manifest themselves in the provider revenue cycle terrain, as well. For example, the OIG is focusing on appropriate and compliant coding and billing practices in the post-acute care environment. There have been a number of high-profile settlements with the OIG concerning inappropriate documentation and coding of higher resource utilization (e.g., therapy time per patient). Additionally, billing and collection policies remain under scrutiny to ensure providers adhere to 501(r) requirements for fair collection protocols, as well as timely identification, quantification and refunding of government overpayments. Also, 2019 will be the first year that home health organizations will be subjected to potential civil monetary penalties for not adhering to new CMS regulations surrounding documentation of the patient’s care plan and utilizing data to ensure continuous improvement of patient care and patient outcomes. Lastly, the Department of Justice has announced a new regional Medicare fraud strike force for the Newark, NJ, and Philadelphia, PA, region. This new taskforce will be the 11th regional joint task force and will focus on prosecuting false claims billing to Medicare, as well as illegally prescribed and distributed opioids and other dangerous narcotics.

Top Risks for 2019

Healthcare

- Regulatory changes and scrutiny may heighten, noticeably affecting the manner in which our products or services will be produced or delivered

- Ensuring privacy/identity management and information security/system protection may require significant resources for us

- Our existing operations and legacy IT infrastructure may not be able to meet performance expectations related to quality, time to market, cost and innovation as well as our competitors, especially new competitors that are "born digital" and with a low cost base for their operations, or established competitors with superior operations

- Our organization’s succession challenges and ability to attract and retain top talent in a tightening talent market may limit our ability to achieve operational targets

- Our organization may not be sufficiently prepared to manage cyber threats that have the potential to significantly disrupt core operations and/or damage our brand

Legend

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Privacy/identity management and information security

A major theme in 2019 will continue to be data privacy and security. The European Union has led the charge with the General Data Protection Regulation (GDPR), which is intended to protect the privacy of individuals within the European Union and the European Economic Area. For healthcare organizations in the United States, the GDPR carries implications that have yet to be truly understood and enforced. The California Consumer Privacy Act is a new state law that imposes GDPR-like privacy protections. It is set to affect the privacy landscape in the next few years as it gives consumers unprecedented control over their personal data. Other states are following suit with their own legislative initiatives. The Health Insurance Portability and Accountability Act (HIPAA) continues to be a major headache for healthcare-covered entities, with penalties for HIPAA violations that have surpassed the $100 million mark. Clearly, the data privacy movement is in full force and organizations will need to increase their resources to meet the demand of complying with regulations and also to prevent penalties as well as reputational damage, as privacy compliance has become required table stakes in the industry.

Identity management continues to be a source of struggle for the healthcare industry. Managing hundreds or even thousands of users that have been introduced into the environment through numerous means (many of whom are not employees, have nonstandard roles, etc.) would place a strain on even the most established and formalized user access management teams. Many healthcare organizations are moving to role-based access, assigning business owners to monitor nonemployees, and implementing requirements for more frequent (e.g., quarterly) review of assigned access rights by supervisors or business owners. However, even with those controls, effectively managing access continues to be of concern.

Another aspect is the need to have strong authentication controls in place for these users to keep this sensitive information private, while not impeding their ability to access key information quickly as they move from patient to patient and potentially workstation to workstation. In a world where phishing and other social engineering tactics to compromise access are rampant, the push for multi-factor authentication (MFA) has hit the forefront of security conversations. Healthcare organizations are trying to find the right balance between securing these accounts and streamlining clinical personnel’s ability to authenticate quickly. Badge tap, proximity badges and biometrics are among security practices being deployed to help with clinicians’ access when physically near a workstation, which is a move in the right direction. While healthcare is making strides in securing access to these workstations, struggles continue with securing access to the multitude of cloud applications in use. Many vendors providing cloud applications, even those providing an electronic health record (EHR) with significant amounts of sensitive data, may not yet offer a MFA option. This allows for any number of attacks on these systems aimed at simply trying to guess passwords, and we are starting to see a number of breaches as a result.

Given the multitude of users, applications that contain sensitive patient information, and numerous reasons why a clinician or hospital employee may need to view data as part of the overall care continuum, the ability to log, monitor and issue alerts on inappropriate user activity that may indicate inappropriate access or snooping into a patient’s information is somewhat like trying to find the proverbial needle in a haystack. There is a focus within many healthcare systems on the activity
within the EHR, but there may be hundreds of other applications containing sensitive information in which user activity is reviewed only when a complaint is submitted or an issue may be expected. Even then, some of these applications do not provide logs of user activity to allow for review, despite the fact that this is a foundational requirement contained in the HIPAA Security Rule.

Healthcare organizations leading in this space are focusing on being able to understand all areas a user could be introduced to the environment, assigning business ownership for user access, utilizing role-based access with specific approval requirements for any standard access deviations, moving away from the use of “set up user A like user B,” rolling out MFA for remote access and cloud applications, enabling some additional authentication functionality for local workstation access, and securing vendor access. As healthcare continues to become more digital and with more third-party vendors playing a part in the patient/consumer service arena, the need for defined processes with appropriate user access technologies will only grow in importance.

Existing operations meeting performance expectations, competing against “born digital” firms

While it came out on June 2, 2017, it doesn’t seem like that long ago when the Health Care Industry Cybersecurity Task Force, established by Congress, issued a draft of its Report on Improving Cybersecurity in the Health Care Industry, which represented an analysis of the state of healthcare cybersecurity in the increasingly interconnected world that has become the reality of today.² What was perhaps most troublesome about the findings outlined in this report was not the improvements needed to keep information confidential or data secure, but rather the 38 references to patient safety compared to 19 references to patient privacy. It is clear that change is needed as the industry continues to rely more heavily on technology and the line continues to gray between care, operations and technology as a result.

One theme identified in the report is that legacy devices are a significant problem in the healthcare industry. The Task Force recommended that the industry take action to “phase out legacy and insecure health care technologies.” In today’s digital world, existing operations and legacy IT infrastructure are a common source of pain and frustration as organizations try to keep up with the competition. Many strategies to further embrace digital transformation die in their infancy because legacy operations and infrastructure are incapable of supporting initiatives such as the use of cognitive computing and advanced analytics, for example. In resource-constrained organizations, the need to advance and evolve is, all too often, overruled by the desire to cut costs and limit spend. A disconnect between the desire at the board level to be recognized at the forefront of technology and a market leader, compared to the budgetary constraints placed on leadership, is a painful reality in many cases.

Recent years have also seen an increase in the opening of virtual care centers. We’ve seen growth in the use of telehealth, resulting in a consumer-friendly level of convenience that patients are seeking. Furthermore, a truly new business threat is emerging as “born digital” companies such as

Amazon, Apple and Google see healthcare as an industry ripe for disruption. These firms are aggressively seeking opportunities to upend healthcare with radical new approaches.

Keeping up with these competitors is a reality that will force many healthcare organizations to take a hard look at increasing their appetite for risk. The need to replace legacy operations and IT infrastructure may soon be a harsh reality that comes along with that cultural shift.

**Succession challenges and ability to attract and retain top talent**

Attracting and retaining top talent remains a key concern for organizations seeking to appropriately plan succession and configure future operational targets. This is particularly true in the healthcare provider space, with expected nursing and physician shortages in the coming years caused primarily by an aging population on the demand side and an anticipated reduction of interest in the medical profession due to increased regulatory scrutiny on the supply side. The prevalence of increasing chronic disease, an aging workforce, especially at top executive levels, and difficulty for non-profit systems to offer competitive compensation for specialized talent in areas such as cybersecurity also add to the complexity of the issue.

With an increasingly diverse workforce and tightening talent market, understanding what driving factors directly attribute to employee attrition should be top priority. One of the first steps in understanding these factors is the development and deployment of a holistic employee retention strategy and program. In tandem, these items not only should seek to determine employees’ top priorities, but also fully engage them in the processes that influence the trajectory of their careers. Effective strategies aid in reducing potential attrition and can also serve as an effective tool in recruiting top-tier talent.

A few items to consider in the development of a comprehensive retention strategy and program include:

- **Compensation transparency**: While compensation in today’s market is not always a strong contributor to attrition, insight and transparency into the organization’s remuneration practices go a long way toward ensuring employees know where they stand against their peers and provide guidance on future potential earnings.

- **Flexible work arrangements**: A noticeable shift toward flexible work arrangements has become a highly demanded perk in today’s marketplace. Allowing employees the flexibility to work remotely and escape the traditional “9 to 5” paradigm are increasingly attractive options. Additionally, these arrangements allow trusted employees to feel valued and empowered, which leads to better long-term contributors.

- **Mentoring**: Employee mentorship programs are another strong factor that should be considered when developing an effective retention strategy. Employees tend to feel more value if they can talk to others to understand the best path for advancement and create an overall course for their careers. Additionally, attrition tends to be higher among employees who are not provided these opportunities.
Cyber threats

The healthcare industry continues to undergo significant change due to the frequency and variety of new technologies being utilized across the care continuum, including devices, applications (on-premises and in the cloud), interfaces, etc. As a result, cyber threats are continuously evolving. But when this technology explosion is coupled with the need for seemingly instant access to sensitive information to provide care and the push for interoperability among many healthcare organizations, the resulting potential exposure expands at a rate with which even the most mature organizations struggle to keep pace. Healthcare organizations are also hindered in dealing with applications and devices that may have known security flaws that cannot be patched, updated or fully retired. Many of these may be the only technology on the market to meet specific healthcare delivery needs for certain care specialties or may have required large capital outlays. They also may involve vendors that have failed to provide and allow for ongoing security updates (as is the case with many medical devices).

A look at the top healthcare industry risks for 2019 presents a sobering picture, as each risk represents a significant issue for any player in the industry group. Each organization’s strategy, business and risk management plans must take these risks into consideration. For example, regulatory changes and scrutiny are on the rise and well up at the top of the list. The cost of staying on top of and responding to regulatory developments continues to increase. Proactive and effective risk management across the identified top risks will be key to maintaining or enhancing enterprise value.

Richard Williams, Managing Director, Healthcare Industry Leader, Protiviti

Attackers are well-aware that data within healthcare organizations has high value from a resale perspective on the black market, where it can be used for any number of fraudulent activities given its depth and detail. This data also makes healthcare organizations prime targets for ransomware attacks given its critical importance as well as its sensitivity. Attackers have developed, utilize and regularly reinvent tactics to pursue this information for monetary gains.

While healthcare organizations are dealing with the ever-expanding use of new technologies along with all of these new attack threats, they are further hindered by a significant shortage in skilled resources that can help address these areas, and likely lack detailed plans for responding to identified incidents, given the necessary amount of near-term priorities and firefighting required of these limited staff.
Those healthcare organizations that are more mature in addressing cyber threats have had success in addressing the technology expansion, with formal governance and assessment processes for new technologies to include connectivity, control and security aspects. Additionally, these organizations are performing ongoing risk analyses, including regular vulnerability scanning and multifaceted penetration testing efforts to identify new areas of vulnerability to be addressed, and have implemented processes and controls to allow for proper incident response and contingency planning should key incidents occur. Healthcare organizations must continue to address the threat landscape presented by the influx of technology from today and tomorrow in order to properly care for patients.

About Protiviti

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of Fortune 1000® and 35 percent of Fortune Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Contacts

Richard Williams
Managing Director, Healthcare Industry Leader
+1.469.374.2469
richard.williams@protiviti.com