The healthy approach to cyber security

For data-intensive healthcare, cyber security is integral to innovation
An oncologist in New York wants to collaborate with colleagues at a European research hospital, but she is concerned about potential HIPAA violations during digital transmission of her patient’s electronic health record.

Hospital administrators are planning to install an array of new medical devices to improve cardiac patient monitoring, but they are worried about introducing new network entry points for cyber-criminals.

A payer is considering a risk-sharing partnership with a physicians’ group, but the deal is waylaid by the group’s approach to securing protected health information (PHI).

Data sharing is believed by many to be the key to the superior care, improved outcomes and lower costs that healthcare consumers and regulatory authorities demand. It is much less expensive to store patients’ medical histories on electronic health records (EHRs) in the Cloud. Diseases can be treated and even cured more expeditiously when doctors are able to search peer-reviewed studies worldwide using cognitive computing. Patient outcomes are improved when doctors can use the Internet of Things to monitor medication adherence and vital signs. Patients in rural and remote areas can gain access to critical medical care in real time via telemedicine technologies.

Digital innovations such as these are poised to take the healthcare industry into the future. However, it is crucial for provider organizations to remember that, for all the opportunities these technologies offer, they also come with significant security and privacy risks.
“The value of digital assets across healthcare is skyrocketing—as are the risks and costs of regulatory non-compliance, reputational damage, and related cyber and privacy breaches,” says Liam Walsh, Principal and Healthcare & Life Sciences Line of Business Leader, KPMG Advisory. “The challenge is to develop an accurate assessment of an organization’s true risk profile and then consciously weigh its genuine risk tolerance against the existing cyber-security investment. I believe many will find that their investments are falling far short.”

Certainly there are strategies, processes and technologies to mitigate a breach once it has occurred. And, according to research by Forbes Insights and KPMG, organizations feel they are making the needed investments in cyber-security programs. However, to mount a truly effective defense, cyber security must become part and parcel of innovation. Effective cyber programs are focused on more than just compliance and threat management but also on the business value cyber can bring to the new approaches, models and capabilities that drive healthcare.

This report outlines key findings from the 2017 KPMG/Forbes Insights Cyber-Security Survey of 100 senior executives from the healthcare field. [One-hundred senior life sciences executives were surveyed as well.] The findings indicate that companies are elevating cyber security to a strategic imperative but at a pace that lags behind their desire to adopt digital technologies to drive innovation. To illustrate, we take a look at the current and desired states of cyber security in healthcare through the lenses of data sharing, vendor management, and medical device implementation. We conclude with our guidance on where organizations should be focusing their efforts.

43% of respondents to KPMG’s survey have not increased their cyber-security budget despite knowledge of recent high-profile breaches

2017 KPMG/Forbes Insights Cyber-Security Survey

“The value of digital assets across healthcare is skyrocketing—as are the risks and costs of regulatory non-compliance, reputational damage, and related cyber and privacy breaches.”

— Liam Walsh, Principal, Healthcare & Life Sciences Line of Business Leader, KPMG Advisory
No matter what happens in the regulatory environment, patient data will remain a critical asset in the healthcare industry. With free-flowing data, providers can focus resources on at-risk patients, improve outcomes, decrease complications, maximize the use of evidence-based protocols, engage in risk-sharing arrangements from accountable care organizations to payer/provider partnerships, and much more.

And yet, there is a dark side to this transformation. As data sharing occurs beyond an organization’s walls, there are cyber-criminals poised to steal valuable PHI. In fact, 47 percent of healthcare firms have had a HIPAA-related security violation or breach in the past two years. This is not surprising, given the widely known fact that medical data is worth at least 10 times as much as financial data on the dark web black market.

As illustrated by our survey findings below, organizations need to elevate data-protection and cyber-security measures to the same level as their knowledge of risks. Those that fail to do so could be subject to immeasurable financial and reputational damage.

1. Sharing and analyzing data

Healthcare organizations place data sharing at the top of their list of perceived vulnerabilities

| Sharing data with third parties | 63% |
| Internet-enabled devices not fully controlled by IT | 59% |
| Lack of resources/budget for effective security programs | 52% |
| External attackers | 50% |
| Employee breaches/theft | 27% |

External bad actors seen as 2x as threatening as internal ones

| External attacker | 72% |
| Phishing-introduced malware | 55% |
| Third-party undetected vulnerability | 43% |
| Internal bad actor | 34% |
| Undetected vulnerability in a system configuration or non-IT-controlled device | 31% |
And yet, there is room for improvement in healthcare’s cyber-security investments:

- **52%** are relying upon cyber insurance to protect their organizations in the event of a cyber-attack.
- **43%** have not increased cyber-security budgets despite recent high-profile breaches.
- **42%** do not plan to increase their cyber-security spending in the next year.
- **34%** have not invested in information security at all in the last year.

2017 KPMG/Forbes Insights Cyber-Security Survey
Healthcare organizations are increasingly seeking vendor partnerships that will help them provide innovative services to patients. However, vendors delivering everything from EHR to revenue cycle software increasingly handle sensitive patient data. To minimize cyber-risks, provider organizations need to be vigilant about ensuring that these vendors have impeccable records. That means no HIPAA violations and an unwavering commitment to cyber-security and privacy methods that align with the provider organizations’ standards.

As the survey data to the right shows, the frequency and methods of assessment providers are using with vendors are encouraging. In fact, 42 percent are conducting assessment on a continuous or monthly basis. However, it is of concern that nearly half of provider organizations surveyed would not re-evaluate a vendor relationship due to a cyber-security vulnerability.
<table>
<thead>
<tr>
<th>Methods of assessment</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Right to audit provisions</td>
<td>66%</td>
</tr>
<tr>
<td>SOC 2/HITRUST certification</td>
<td>43%</td>
</tr>
<tr>
<td>Survey of third parties</td>
<td>40%</td>
</tr>
<tr>
<td>Contract with unlimited liability</td>
<td>37%</td>
</tr>
<tr>
<td>Analysis of publicly available information</td>
<td>32%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cyber-event driving a change in vendor relationship</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>47%</td>
</tr>
<tr>
<td>Frequent HIPAA issues</td>
<td>25%</td>
</tr>
<tr>
<td>Malware attack</td>
<td>24%</td>
</tr>
<tr>
<td>Insufficient safeguards over protected information</td>
<td>22%</td>
</tr>
<tr>
<td>Ransomware attack</td>
<td>7%</td>
</tr>
</tbody>
</table>
3. Addressing medical device security

Wireless, sensor-based medical devices are viewed as one of the most significant innovations in healthcare. They allow seamless patient management, efficient communication, and early intervention. And yet, these devices have the potential to be both a blessing and a curse. From harming patients with device tampering, to using a medical device as an entryway to a hospital’s network, to gaining inappropriate access to sensitive information, cyber-criminals see opportunities in these increasingly ubiquitous devices.

When it comes to the new generation of software-enabled medical devices, the entire manufacturer and provider ecosystem must work together to strike a balance between strong cyber-security measures on the one hand, and the ability to treat patients rapidly in an emergency and improve their health outcomes over time on the other.

Although our survey results should spark some optimism when it comes to organizations’ willingness to collaborate and perform regular security testing, there is still room for improvement when it comes to establishing formal programs. Despite the fact that more than 77 percent of healthcare organizations have seen a device breach in recent years, most are more focused on identifying an attack after it has taken place than on managing risks proactively. Preventive measures are particularly critical with older medical devices, even if they have been retrofitted with more modern cyber-security capabilities.

Collaborating with medical device manufacturers

<table>
<thead>
<tr>
<th>Security testing methods</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security hardening standards</td>
<td>71%</td>
</tr>
<tr>
<td>Vulnerability scanning</td>
<td>67%</td>
</tr>
<tr>
<td>Network segmentation</td>
<td>65%</td>
</tr>
<tr>
<td>Software and firmware</td>
<td>64%</td>
</tr>
<tr>
<td>Configuration management database</td>
<td>64%</td>
</tr>
<tr>
<td>Penetration testing</td>
<td>48%</td>
</tr>
</tbody>
</table>

2017 KPMG/Forbes Insights Cyber-Security Survey
Organizations need to find a balance

87% can identify a cyber-event

Only 59% manage risk proactively

WHAT TO DO NOW: Provide input to device manufacturers in the design stage

“Healthcare has been working with connected devices for many, many years; they were an early adopter. But that can be a double-edged sword. Now, so many in healthcare are burdened with older processes and technologies. The legacy systems that once conferred early advantage and benefits are now making it more difficult for them to address emerging cyber-risks.

“Partnering with device manufacturers on risk mitigation during the technology development stage is critical to safely using innovative medical devices to treat patients.”

— Phil Lageschulte, Partner, Emerging Technology Risk Network Leader, KPMG Advisory
4. Creating a balanced cyber-security program

Formal processes and continuous technology assessment are critical to cyber security. However, organizations should remember that people issues cannot be an afterthought. In fact, technologies are only as good as the people and processes put in place to manage and monitor them.

As the survey data in the following pages illustrates, there is room for improvement in both the process and the technology approaches to cyber security. However, it is of the greatest concern that only 24 percent of healthcare organizations are making investments in staff. This is a far cry from the 82 percent focused on stronger processes and the 79 percent investing in more sophisticated technology protections, such as encryption and firewalls.

Processes

In the overwhelming majority of cases, healthcare organizations report they have the right processes in place to battle cyber-attacks after they’ve occurred. And, there has been a significant commitment to investigative and forensic cyber programs. It is of concern, however, that most of these efforts are reactive, as opposed to preventive measures taken before vulnerable technologies are put in place.

**Cyber-security investments**

- Stronger policies/controls: 82%
- Advanced technology: 79%
- Governance: 49%
- Managed services: 47%
- Consulting: 41%
- Hardware: 28%
- Staff: 24%

2017 KPMG/Forbes Insights Cyber-Security Survey

**Reactive measures**

- Incident response plan: 95%
- Security operations center (SOC): 85%
- Business continuity plan: 82%
- Internal and external investigative and forensic resources: 43%

2017 KPMG/Forbes Insights Cyber-Security Survey
WHAT TO DO NOW: Evaluate the effectiveness of their controls from a return on investment perspective

“It’s not enough for companies to apply security controls to simply check a box or receive a passing grade on a maturity assessment. Organizations need to evaluate the effectiveness of their controls from a return on investment perspective, focusing on the cost of data loss from a control failure against the cost associated with the people, process or technology involved in implementing the control itself. More and more organizational leadership focus will emphasize reliable measurement techniques and criteria for determining the value of security in protecting sensitive healthcare data.”

— Carl Kriebel, Managing Director, KPMG Cyber Security Services
In healthcare, a great deal of the technology that facilitates innovation, such as electronic health records, the Cloud and clinical-decision making tools, also introduce the most risk. Armed with awareness of these new potential attack vectors, bad actors are increasing their focus on healthcare organizations and expanding their methods of infiltration. Although implementing advanced technologies is critical to growth in healthcare, it is of the utmost importance that organizations prioritize and address vulnerabilities before new technologies are integrated.

Perceived risk of new innovations:

- **53%** Computer physician order entry/EHRs
- **53%** Software
- **49%** Cloud computing
- **46%** ASP apps
- **38%** Clinical decision-making tools
- **27%** Clinical diagnostic hardware
- **25%** Cloud services
- **22%** Mobile devices

2017 KPMG/Forbes Insights Cyber Security Survey
“The days of protecting yourself against everything all the time are long gone. Cyber threats and bad actors are evolving at a pace that is virtually impossible to get ahead of. Forward thinking organizations are focused on identifying their most valuable assets – their crown jewels – and applying appropriate cyber controls so that scarce resources are applied in the most impactful way. By focusing on crown jewel assets, cyber security can become an enabler allowing organizations to achieve their business objectives.”

— Fred Rica, Principal, KPMG Cyber Security Services

### WHAT TO DO NOW: Prioritize defending high value assets

<table>
<thead>
<tr>
<th>Methods of attacks</th>
<th>72%</th>
<th>47%</th>
<th>32%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal theft/negligence</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ransomware</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2017 KPMG/Forbes Insights CyberSecurity Survey

Healthcare and cyber security 11
People

Healthcare organizations are aware that internal staff present significant risks. More than half of the organizations surveyed have seen a data breach resulting from an employee falling prey to a phishing scam, and more than a third have had information stolen from internal databases by a disgruntled employee. Training on prevention and detection would help mitigate these internal risks. And yet, 36 percent do not have a chief information security officer (CISO) and, as illustrated below, most are not providing cyber-security training on a regular basis.

Frequency of cyber-security training

<table>
<thead>
<tr>
<th></th>
<th>Providers</th>
<th>Payers</th>
</tr>
</thead>
<tbody>
<tr>
<td>As needed</td>
<td>36%</td>
<td></td>
</tr>
<tr>
<td>On a quarterly basis</td>
<td>34%</td>
<td>60%</td>
</tr>
<tr>
<td>On an annual basis</td>
<td>34%</td>
<td>60%</td>
</tr>
</tbody>
</table>

Origination of data loss or system compromise

55% have seen an employee falling prey to phishing scam

34% have seen theft from secured database by internal bad actor

2017 KPMG/Forbes Insights Cyber-Security Survey
WHAT TO DO NOW: Put a laser focus on staff training

“The healthcare industry depends on people: skilled doctors, well-trained nurses, visionary administrators, and responsive support personnel. Relegating staff issues to a sidebar in the cyber-security discussion is a mistake. Organizations must take a coordinated approach involving implementation of the latest cyber technologies, continuously re-imagined policies and procedures, and regular training of staff at all levels. Shortchanging any one of these elements raises the risk of unimaginable damage to an organization’s reputation and ability to attract and serve patients.”

— Dion Sheidy, U.S. Healthcare Advisory Leader
Conclusion: Building a cyber-security-focused culture
The healthcare industry is evolving toward a true value-based system, seeking to elevate both individual and population health outcomes, and assuming responsibility for complex quality measures. This requires digital technologies that allow data to flow freely. However, for every step forward organizations take, cyber-criminals are progressing right alongside them with ever more aggressive means of system infiltration and data theft.

Organizations who ignore this reality are opening themselves up to unfathomable damage to their reputations, their finances and even their viability. From our perspective, a mindset shift must occur so that cyber security is viewed as an enabler of innovation. Whether organizations are focused on internal risks, risks associated with partners and vendors, or risks arising from insufficient people, technology and procedural resources, addressing cyber security should be inseparable from pursuing growth.

“Many organizations believe they can address cyber security through a focus on technology alone,” concludes Liam Walsh. “However, if they are going to pursue an aggressive innovation agenda, it’s equally important to create a pervasive culture of cyber security, and that starts with people.

“More than a third of healthcare organizations don’t even have a CISO. You can have great technology for detection and response, but, if you don’t have the right people in place, empowered and engaged, organizations cannot correctly calibrate processes and focus efforts on the right risks and assets.

“Just as the most successful healthcare leaders are weaving innovation into the fabric of their organizations, a cyber-security mindset must be equally entrenched. Pursuing disruptive innovation without cyber security is like tightrope walking without a net.”
This cyber-security report is based on two separate surveys: one for healthcare payers and providers and a second for life sciences, which includes pharmaceutical makers, biopharma and medical device makers. A total of 200 executives were polled, 100 from each from these two core groups. Though many of the questions were asked of both sectors, others are unique to either the individual healthcare or life sciences samples. The survey data was analyzed by KPMG and fielded by Forbes Insights.

### Healthcare Sector (100 executives)

- **Title**: 20 Chief Technology Officer, 30 Chief Information Officer, 22 Chief Information Security Officer, 29 Chief Security Officer
- **Annual Revenue**: 50 Over $10 billion, 50 $5 billion to under $10 billion, 50 $2 billion to under $5 billion, 50 $500 million to under $2 billion

### Life Sciences Sector (100 executives)

- **Title**: 1 Biopharma/pharma, 1 Medical devices
- **Annual Revenue**: 50 Over $10 billion, 50 $5 billion to under $10 billion, 50 $2 billion to under $5 billion, 50 $500 million to under $2 billion
KPMG’s Cyber-Security Services practice assists organizations in transforming their security, privacy and business continuity controls into business- and innovation-enabling platforms. We view security as a process, not a solution. Therefore, safeguarding IT networks and sensitive data from electronic attack should allow organizations to take control of uncertainty and turn risk into advantage. In particular, our clients are able to take cyber security to the next level and use it as a means to transform the enterprise.

Our teams have significant on-the-ground credentials in the cyber-security space, from pre-breach to post-breach, having been retained by some of the world’s largest organizations in life sciences, healthcare and other industries. Our work runs the gamut from strategy and governance, to large-scale security transformation programs, to a full range of cyber-risk and response services, including on-demand malicious code analysis, host- and enterprise-based forensics, network forensics, threat intelligence, and expert testimony.

KPMG Cyber Response Services professionals have experience working on all forms of cyber-crime, including insider threats, data breaches, hacktivism, and advanced persistent threat intrusions. On top of this foundation, KPMG has developed a proprietary cyber-security process refined through real-world experience and a focus on actionable results, rules of evidence, and intensive on-going security testing.
Contact us

Liam A. Walsh  
Healthcare & Life Sciences Line of Business Leader, KPMG Advisory  
KPMG LLP  
773-230-0171  
lawalsh@kpmg.com

Carl Kriebel  
Managing Director, Cyber Security  
KPMG LLP  
412-208-8716  
ckriebel@kpmg.com

Fred Rica  
Principal, Cyber Security  
KPMG LLP  
973-912-4524  
frica@kpmg.com

Dion Sheidy  
U.S. Healthcare Advisory Leader  
KPMG LLP  
615-248-5519  
dsheidy@kpmg.com

Phil Lageschulte  
Partner, Emerging Technology Risk Network Leader, KPMG Advisory  
KPMG LLP  
312-665-5380  
pjlageschulte@kpmg.com

To learn more about our Healthcare & Life Sciences practice and capabilities, visit us at www.kpmg.com/us/healthcarelifesciences

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2019 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved. Printed in the U.S.A. The KPMG name and logo are registered trademarks or trademarks of KPMG International.