KPMG

The healthy approach to cyber security

For data-intensive healthcare, cyber security is integral to innovation

kpmg.com

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.

KPMG

"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."

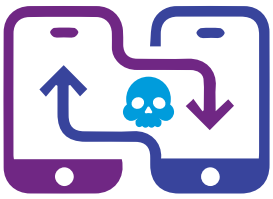
— Liam Walsh, Principal, Healthcare & Life Sciences Line of Business Leader, KPMG Advisory

1. Sharing and analyzing data

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.



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%

2017 KPMG/Forbes Insights Cyber-Security Survey

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%

2017 KPMG/Forbes Insights Cyber-Security Survey

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

WHAT TO DO NOW: To get value from data, make cyber security an urgent priority

"Healthcare runs on thin margins, often just two to four percent. So, when CIOs are told that addressing cyber-risk will take a much larger investment, the reaction, increasingly, is to simply resign themselves to accepting greater risk. That's not the right answer.

"Yes, top resources in cyber security do not come cheap. But healthcare is only now in the beginning phases of becoming one of the most data-intensive industries imaginable, which makes it one of the most susceptible to cyber-risks. The investments will hit margins. But the industry as a whole needs to revisit core processes to balance getting value out of data with minimizing risk – starting yesterday."

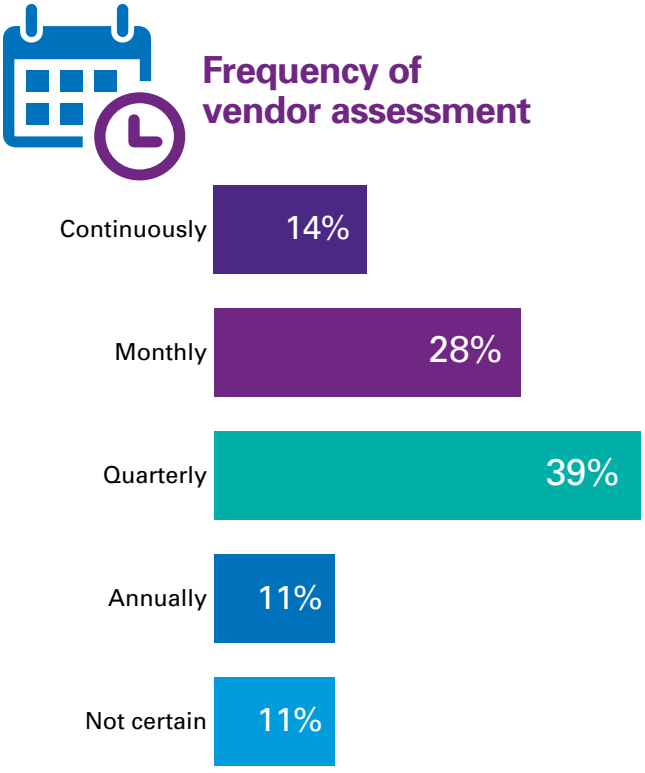
— Michael Ebert, Partner, KPMG Cyber-Security Services

2. Choosing vendors

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.

Frequency of vendor assessment



2017 KPMG/Forbes Insights Cyber-Security Survey

Methods of assessment

Right to audit provisions	66%
SOC 2/HITRUST certification	43%
Survey of third parties	40%
Contract with unlimited liability	37%
Analysis of publicly available information	32%

2017 KPMG/Forbes Insights Cyber-Security Survey

Cyber-event driving a change in vendor relationship

None	47%
Frequent HIPAA issues	25%
Malware attack	24%
Insufficient safeguards over protected information	22%
Ransomware attack	7%

2017 KPMG/Forbes Insights Cyber-Security Survey

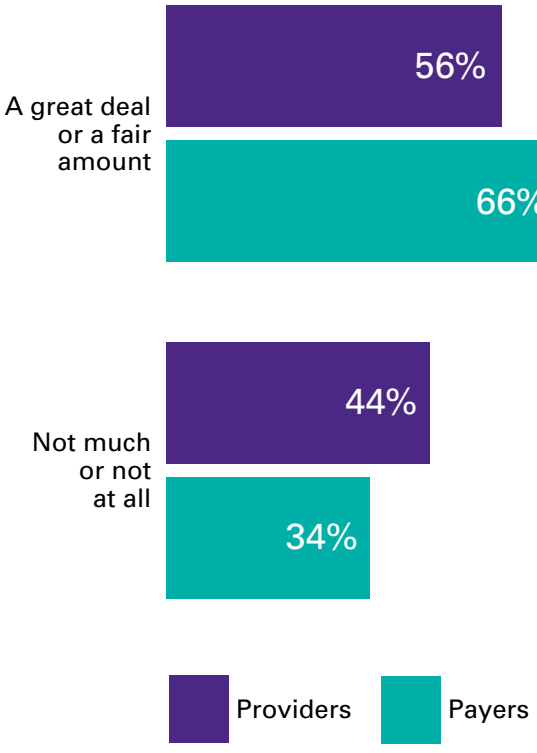
3. Addressing medical device security

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.

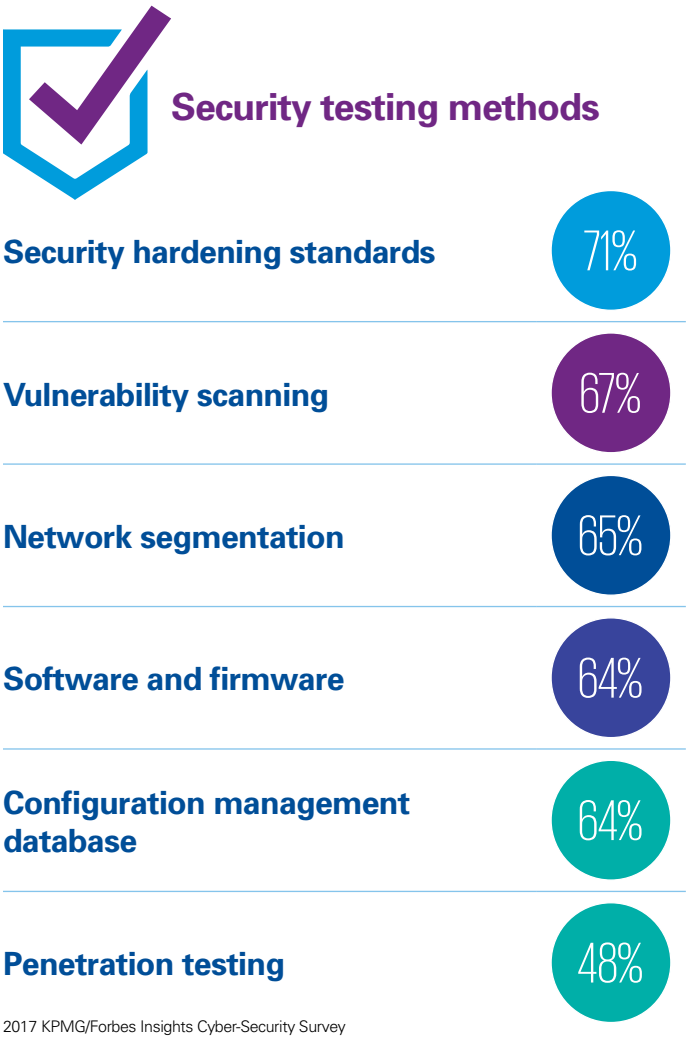
Although our survey results should spark some optimism when it comes to organizations' willingness to collaborate and perform regular security testing, there is still room for improvement when it comes to establishing formal programs. Despite the fact that more than 77 percent of healthcare organizations 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



2017 KPMG/Forbes Insights Cyber-Security Survey

Security testing methods



2017 KPMG/Forbes Insights Cyber-Security Survey

Organizations need to find a balance

87% can identify a cyber-event

Only 59% manage risk proactively

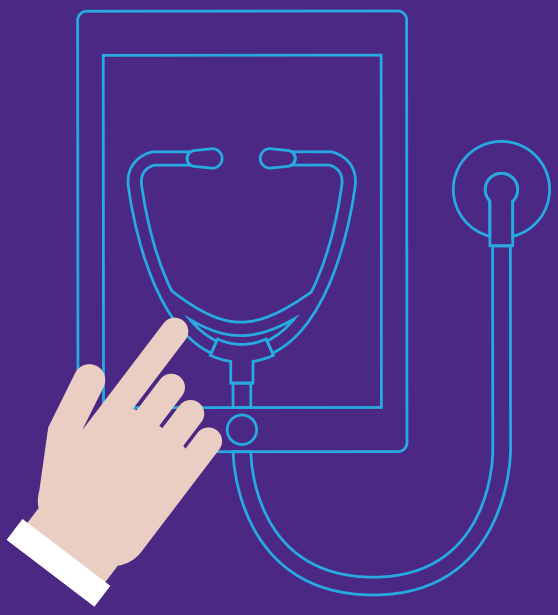
2017 KPMG/Forbes Insights Cyber-Security Survey

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

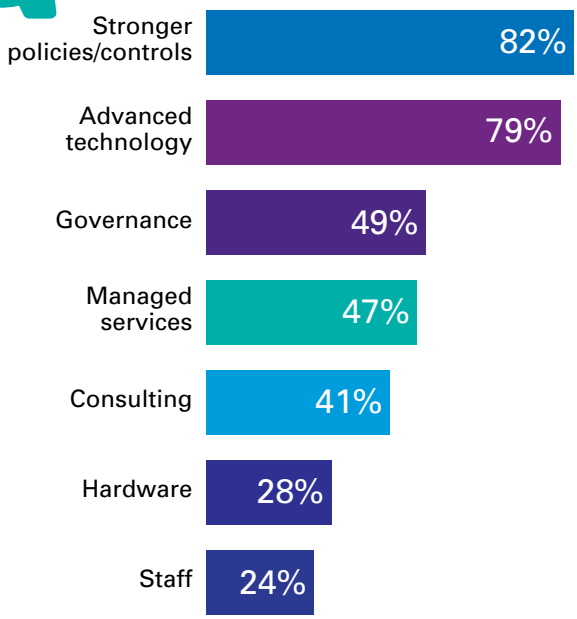


4. Creating a balanced cyber-security program

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.

Cyber-security investments



2017 KPMG/Forbes Insights Cyber-Security Survey

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.

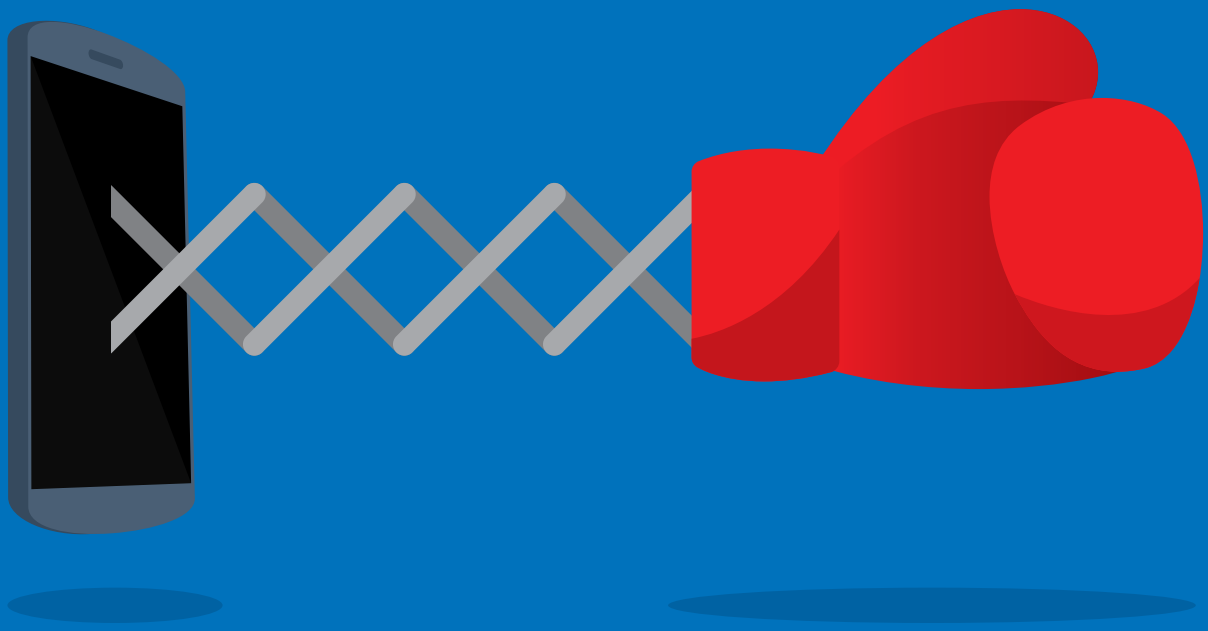
Reactive measures

2017 KPMG/Forbes Insights Cyber-Security Survey

WHAT TO DO NOW: Transition from a reactive to a proactive defense

"Organizations have become a bit complacent about the real consequences of cyber-threats. Addressing risk with reactive forensic measures doesn't protect patients. Senior management must foster a culture of cyber security that is intertwined with innovation. And the message must come from the top that cyber security—just like innovation—is part of everyone's job description."

— Mark Johnson, Managing Director, KPMG Cyber-Security Services



Technology

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

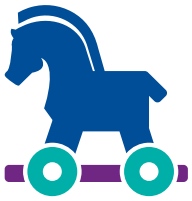
38% Clinical decision-making tools

27% Clinical diagnostic hardware

25% Cloud services

22% Mobile devices

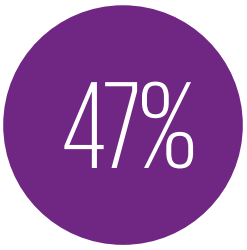
2017 KPMG/Forbes Insights Cyber-Security Survey



Methods of attacks

2017 KPMG/Forbes Insights Cyber-Security Survey

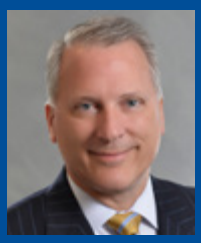
Malware



Internal theft/negligence

Ransomware

WHAT TO DO NOW: Educate yourself on where the greatest IT risks lie



"Healthcare finds itself in a very dangerous period with regard to cyber-risks. Over the past few years, the focus has been on electronic health records, in many cases draining resources and investment from broader IT and cyber-security efforts. Recent findings from the federal Healthcare Cyber Security Taskforce support KPMG's perspective that IT investments are missing the mark on cyber while remaining overly focused on EHRs.

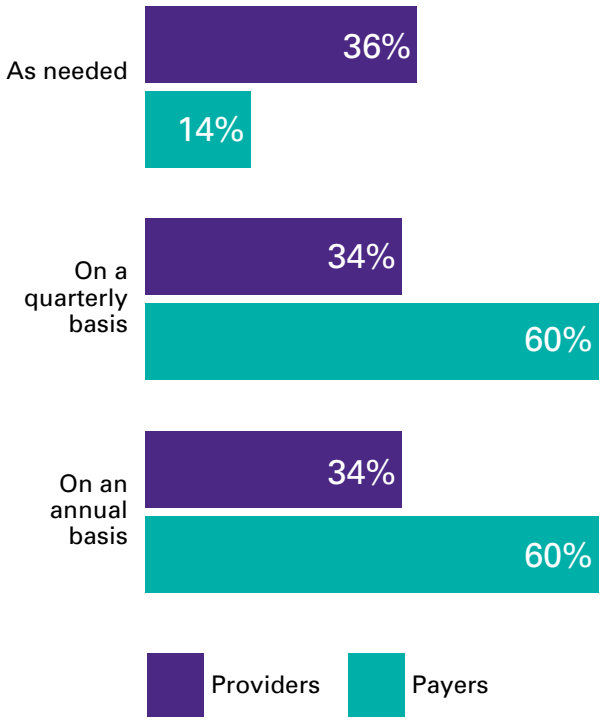
"Meanwhile, bad actors have been continuously improving their own craft. So, it would not be surprising if the number and severity of assaults and breaches reaches a high point. Organizations need to educate themselves on where the greatest risks lie."

— Michael Ebert, Partner, KPMG Cyber-Security Services

People

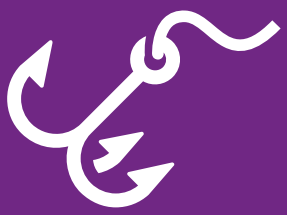
Healthcare organizations are aware that internal staff present significant risks. More than half of the organizations surveyed have seen a data breach resulting from an employee falling prey to a phishing scam, and more than a third have had information stolen from internal databases by a disgruntled 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



2017 KPMG/Forbes Insights Cyber-Security Survey

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.

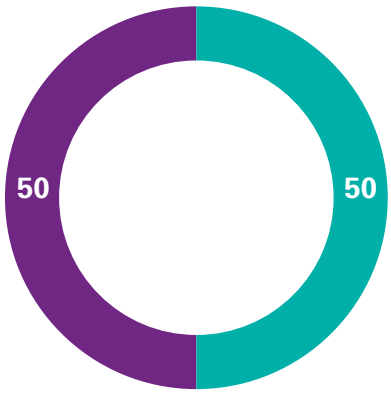
"More than a third of healthcare organizations don't even have a CISO. You can have great technology for detection and response, but, if you don't have the right people in place, empowered and engaged, organizations cannot correctly calibrate processes and focus efforts on the right risks and assets.

"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."

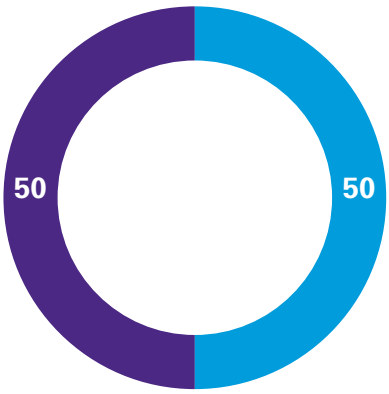
Methodology

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.

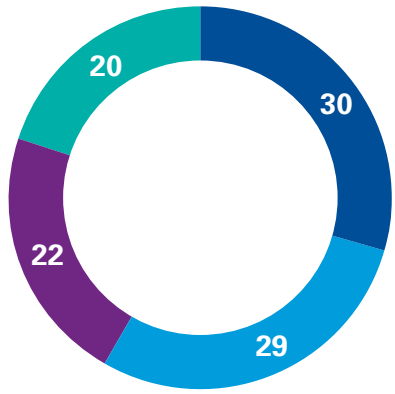
Healthcare Sector (100 executives)



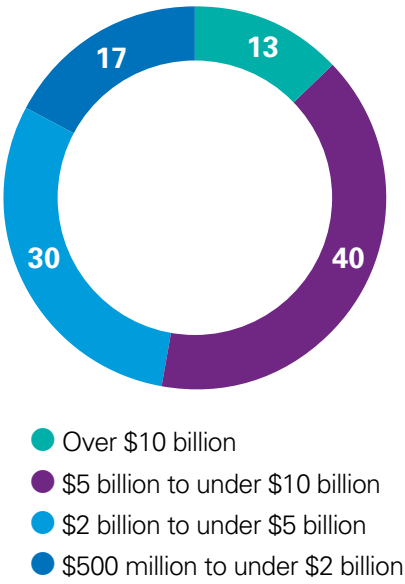
Life Sciences Sector (100 executives)



Title (200 executives)



Annual Revenue (200 executives)



How KPMG can help

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

Michael Ebert
Partner, KPMG Cyber-Security Services
KPMG LLP
267-256-1686
mdebert@kpmg.com

Mark Johnson
Managing Director, KPMG Cyber-Security Services
KPMG LLP
615-248-5548
mmjohnson@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.

kpmg.com/socialmedia