KPMG
cutting through complexity

HEALTH CARE AND CYBER SECURITY:

Increasing Threats Require Increased Capabilities

kpmg.com

EXECUTIVE SUMMARY

Four-fifths of executives at healthcare providers and payers say their information technology has been compromised by cyber-attacks. At the core of the increased risk to healthcare organizations is the richness and uniqueness of the information that the health plans, doctors, hospitals and other providers handle. Apart from typical financial fraud, there is also the possibility of medical insurance fraud, or, in the case of providers, attacks on computer-controlled medical devices. As this is the largest part of the U.S. economy and a safeguard of peoples' well-being, healthcare is a matter of national security.

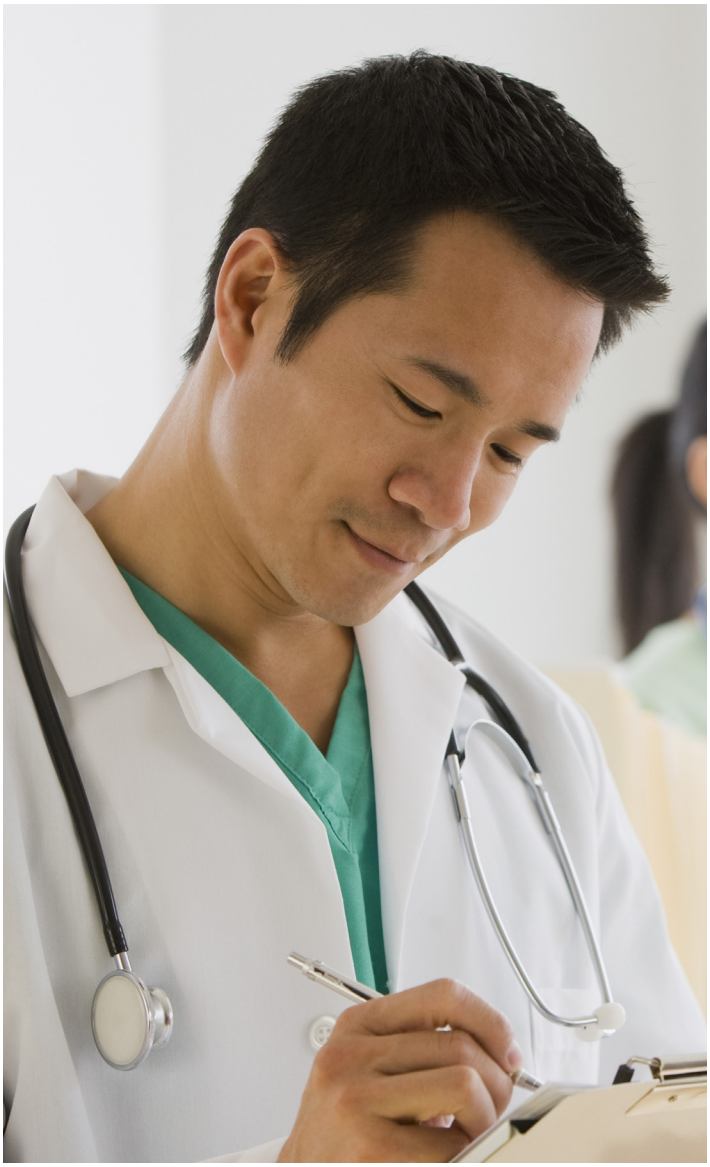
Despite such significant repercussions of a cyber-attack, the healthcare sector lags in terms of its preparedness for cyber threats. As recent events have made clear, protecting information is not easy. Hackers will find opportunities to exploit flaws in the way healthcare organizations currently fund, manage, enable, organize and implement their information protection capabilities.

In terms of technical capabilities, the healthcare industry is behind other industries in protecting its infrastructure and electronic protected health information (ePHI) – as commonly seen in the use of outdated clinical technology, insecure network-enabled medical devices, and an overall lack of information security management processes.

Based on our experience, healthcare organizations are facing increased security threats by:

- The **adoption of digital patient records** and the automation of clinical systems.
- The use of **antiquated EMR and clinical applications** that are not designed to securely operate in today's networked environment and software vendors who push that problem to the provider.
- The **ease of distributing ePHI** both internally (laptops, mobile devices, thumb drives) and externally (third parties, Cloud services).
- The **heterogeneous nature** of networked systems and applications (i.e. network-enabled respirator pumps on the same network as registration systems that can browse the Internet).
- The **evolving threat landscape,** where cyber-attacks today are more sophisticated and well-funded given the increased value of the compromised data on the black market.

Some organizations may not realize the sophistication of hackers and their means to infiltrate confidential patient data networks. Interconnectivity of data in healthcare holds huge promise for health outcomes – improving both quality and efficiency of medicine. The risks associated with interconnectivity are also great, however. The nature, depth and consequences of cyber-attacks in healthcare have all changed, and the approach to containing those threats has to change and align with a healthcare organization's objectives, as well.

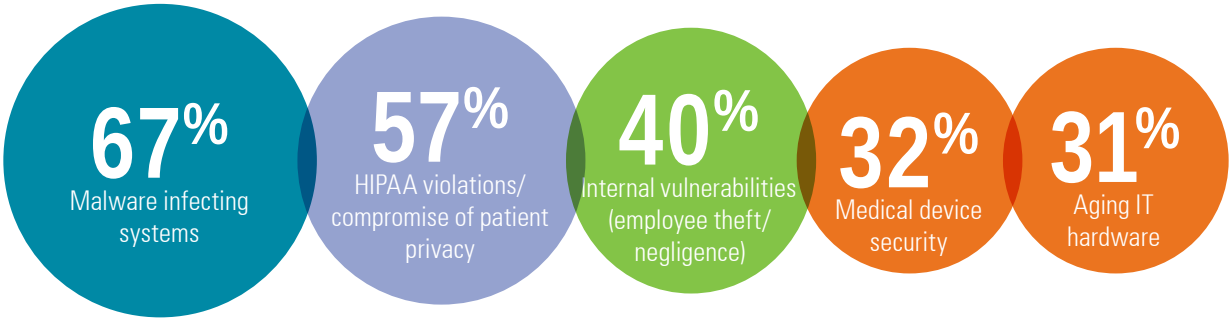


TOP CYBER SECURITY THREATS

The most important cyber security concerns for healthcare providers and payers are coming from external sources, according to KPMG's survey of 223 healthcare executives, who named external attackers and third-parties as their top vulnerabilities. The top threats are malware and HIPAA violations. (See charts.)

GREATEST VULNERABILITIES IN DATA SECURITY

TOP INFORMATION SECURITY CONCERNS



"The richness of the information means that the cyber security threat to healthcare has increased," says Michael Ebert, KPMG partner and healthcare leader at the firm's Cyber Practice. "The magnitude of the threat against healthcare information has grown exponentially, but the intention or spend in securing that information has not always followed."

As a result of divergent priorities, payers and providers have differing concerns when it comes to security breaches. For providers, regulatory enforcement issues or litigation can cut into already thin profit margins. "A hospital typically has some tough choices when it comes to investing," Ebert says. "If it has a million dollars it is more likely to spend on patient care and saving lives before protecting their data."

Payers tend to be larger, publicly traded organizations that operate in multiple jurisdictions. Their main concerns are a financial loss that could affect shareholders or a reputational impact that could dampen growth plans. (See charts.)

TOP CONCERNS FOR PROVIDERS	
Regulatory enforcement	50%
Litigation	45%
Financial loss	44%
Reputation	39%
Job security	6%

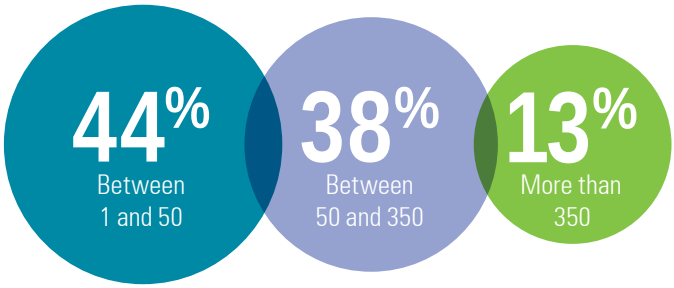
TOP CONCERNS FOR PAYERS	
Financial loss	57%
Reputation	46%
Litigation	38%
Regulatory enforcement	35%
Job security	3%

FREQUENCY OF CYBER SECURITY BREACHES

KPMG's survey shows that healthcare organizations are on the high end of the spectrum when it comes to cyber-attacks. They are not as frequently targeted as the financial services sector, which has spent the last 20 years focusing on cyber security and protection.

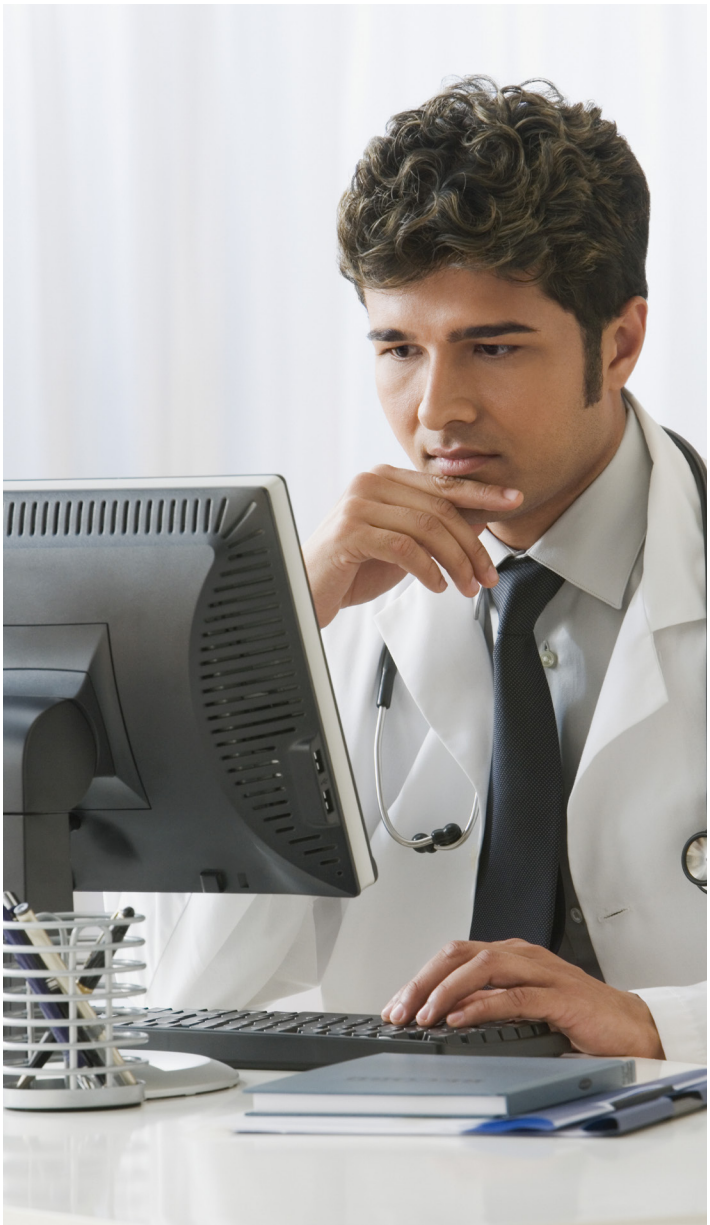
Of increased concern is the respondents' attempts to track cyber threat attempts. Just 13% of KPMG's survey respondents reported tracking more than once-a-day known attempts at a cyber security breach. (See chart.)

NUMBER OF CYBER THREAT ATTEMPTS TRACKED IN THE LAST 12 MONTHS



This is indicative of organizations not understanding, tracking, reporting and managing threats effectively. Mature incident and vulnerability management processes are lacking in most organizations, and thus, daily threats aren't even reported or managed effectively by many organizations. One KPMG client saw a 1000% increase in incidents and vulnerability reporting to their enterprise once they implemented an effective Security Operations Center (SOC) to intercept, interpret, and report on threats.

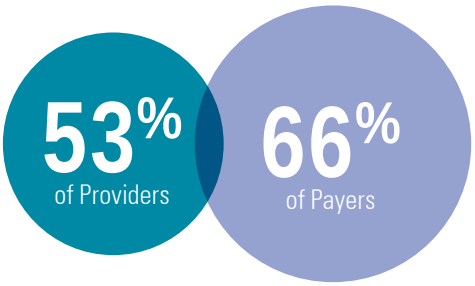
Ebert suspects that a large percentage of the organizations are underreporting security threats as well. "They are probably compromised and don't even know it," he points out. In fact, 25% of respondents surveyed by KPMG say that, based on their organization's current protection systems, they don't have or don't know their capabilities, in real time, to detect if their organization's systems are being compromised.



HOW CYBER SECURE ARE HEALTHCARE ORGANIZATIONS?

While a majority of organizations consider themselves prepared for defense against a cyber-attack, they may be overconfident about their capabilities, says KPMG's Cyber Practice. (See chart.)

CONSIDER THEMSELVES READY TO DEFEND AGAINST A CYBER-ATTACK



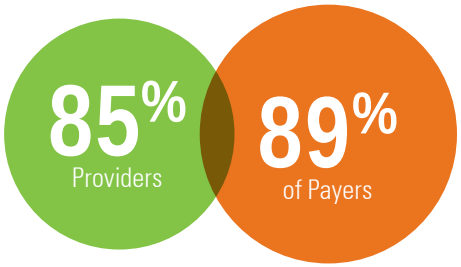
Instant management and instant response are very delicate matters that involve investigating, tracking and eliminating cyber threats, as well as communicating and reporting threats to the public and regulatory bodies.

Some organizations may hurt themselves by reporting breaches almost too quickly, before they understand where the threat is coming from, who the attacker is and which parts of the system have been compromised, Ebert says. "It's important to understand the attack's total footprint and how it's spreading before shutting it down. Otherwise an organization will not be able to prevent it from spreading or properly contain the attack," he added.

CYBER-ATTACK PREPARATION IS KEY

The KPMG survey reveals that, while the discussion around cyber security is occurring in executive suites (See Chart), many healthcare organizations have not yet taken all the necessary steps to prepare their organizations for cyber security threats. (See Box)

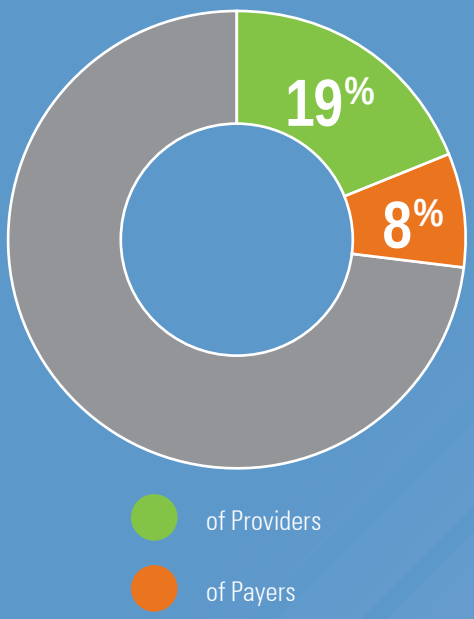
CYBER SECURITY HAS BEEN DISCUSSED AT THE BOARD LEVEL IN THE PAST YEAR



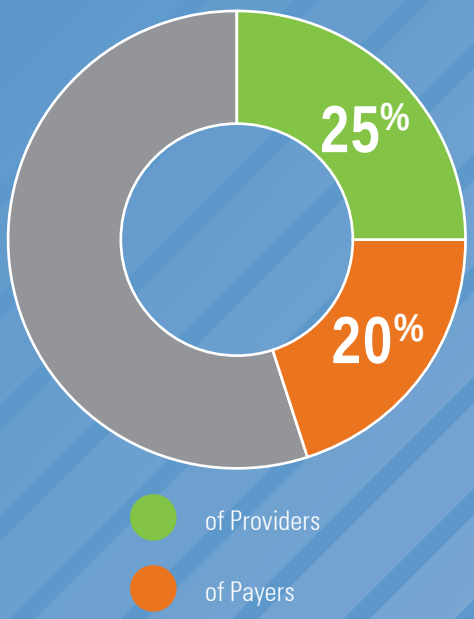
NOT EVERY HEALTHCARE ORGANIZATION IS PREPARED FOR CYBER-ATTACKS

In terms of human capital, almost one-fifth of healthcare providers don't have a leader solely responsible for information technology security, versus 8% of payers. (See Chart) The starting point of building a cyber security team should be appointing somebody responsible solely for information security, says Greg Bell, who leads KPMG's U.S. Cyber Practice. However, 23 percent of organizations do not have a security operations center to identify and evaluate threats.

DO NOT HAVE A LEADER SOLELY RESPONSIBLE FOR INFORMATION SECURITY



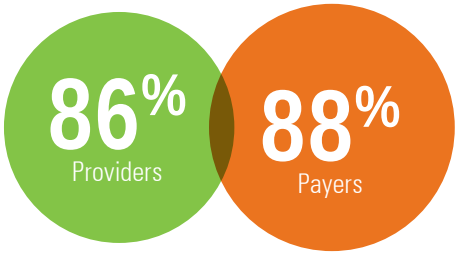
DO NOT HAVE INFORMATION SECURITY OPERATIONS CENTER



WHAT IS THE RIGHT INVESTMENT IN CYBER SECURITY?

While the majority of organizations surveyed by KPMG increased their spending on cyber security and invested in cyber security over the last 12 months, the investment has not resulted in adequate security in many areas. (See charts.) "That spending rate is probably underinvested considering that the threat to an organization has increased so much," says Ebert.

MY ORGANIZATION INVESTED IN INFORMATION SECURITY DURING THE PAST 12 MONTHS



MY ORGANIZATION HAS ADEQUATE IT SECURITY RESOURCES FOR THE FOLLOWING AREAS

IT compliance/risk management	70%
Managing firewalls and other critical network resources	60%
Handling security incidents	55%
Monitoring data leakage	53%
Monitoring technical infrastructure resources for health and welfare	49%
Managing vendor security risks	35%

This discrepancy between levels of investment in cyber security and capabilities is also the direct result of an ad hoc approach to building security into the networks, which boils down to uncoordinated buying. "If spending on security is not part of a cohesive, coordinated strategy, those expenditures tend to be more wasteful than beneficial," warns Bell.

CONCLUSION

With the changing nature, depth and consequences of cyber-attacks in healthcare, the nature of preventing, monitoring and managing those threats requires a new approach, based on:

Incorporation of cyber security in the technology and network architecture upfront, via strategic design. Since many organizations achieved their interconnectivity by evolution, resulting in inadequate controls, what is in many cases required today is a redesign and development of a security implementation plan. Investment in security needs to become part of a cohesive, coordinated digital strategy.

A well-prepared and coordinated cyber security team and a security operations center. A successful approach requires appointing an executive with sole responsibility over cyber security, as well as capabilities for instant monitoring. Other areas that need to be covered include managing the breach itself and communicating with various constituencies.

Increased cyber security awareness and capabilities at all levels. Cyber security is a business risk as well as a technology risk. Thus cyber security executives need to be equally conversant in both. While the executive involvement typically boils down to the awareness component, it is important to have board members savvy about cyber security and able to help management in this area.

Taking a broad view of the organization when implementing cyber security. By working with a variety of business partners, organizations have, in effect, become extended value chains. The third-party vector poses an increased cyber security risk. It is crucial to understand the inherent risk of having multiple third-parties engaged and to identify risks that have to be remediated.

METHODOLOGY

This report is based on data from a survey of 223 U.S.-based healthcare executives, conducted by Forbes Insights. Fifty-six percent came from for-profit organizations, and 44% from the not-for-profit sector. All had revenues of at least $500 million; 70% had revenues over $1 billion.

Greg Bell
KPMG Cyber US Leader
T: +1 404 222 7197
E: rgregbell@kpmg.com

Michael Ebert
KPMG Cyber Healthcare and Life Sciences Leader
T: +1 267 256 1686
E: mdebert@kpmg.com

kpmg.com