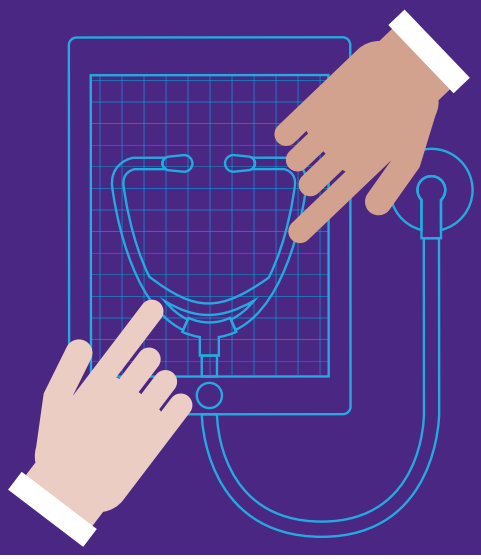
Is teaming the key to medical device cyber security?



Manufacturers and providers must collaborate to contain cyber-risks as device functionality flourishes

Jim, who suffers from sleep apnea, gets up on a Saturday morning, checks his smart watch to see how many hours of productive REM sleep he got, and transmits the data to a cloud-based app that stores information his sleep doctor can analyze. Then, before he even wakes up his daughter, who has Type 1 diabetes, he checks her continuous glucose monitor and sends the overnight results to her endocrinologist. Later that weekend, another wearable biosensor alerts him to the fact that his blood oxygen levels are a bit low, and he has a low-grade fever. He goes to see his doctor, discovers that he is positive for early signs of the flu, and starts a course of anti-viral medication to minimize his symptoms. A week later, he goes to visit his elderly mother, who is in a rehabilitation center following cardiac surgery, and marvels at the wireless accelerometry monitor that provides her surgeons with up-to-the-minute details of her post-surgery mobility.

Although some of the medical devices in this scenario are still in the development phase, it is clear that connected devices are central to healthcare's future. With real-time symptom monitoring and data sharing, wireless, sensor-based medical devices make for seamless self-management, efficient communication with providers, and early intervention.

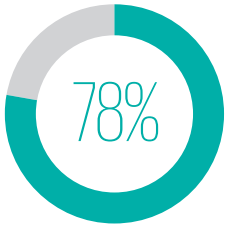
And yet, these devices have the potential to be both a blessing and a curse. While the mobility of medical data enhances healthcare providers' ability to treat patients and improve outcomes, these same features also introduce the risk of cyber-security threats and data privacy issues. From harming patients 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.

Since both manufacturers and provider organizations have a vested interest in using advanced medical devices to improve patient health, a collaborative approach to cyber security and privacy is imperative. Organizations seem to be moving in this direction but not quite fast enough to stay ahead of potential attacks, as evidenced by findings from a recent cyber-security survey from Forbes Insights and KPMG.

Since both manufacturers and provider organizations have a vested interest in using advanced medical devices to improve patient health, a collaborative approach to cyber security and privacy is imperative.

The provider perspective

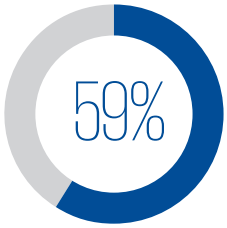
Cyber-attacks on medical devices are no longer fiction. More than 75 percent of both providers and payers have had a medical device breach in the last few years, according to the KPMG/Forbes survey.



Providers

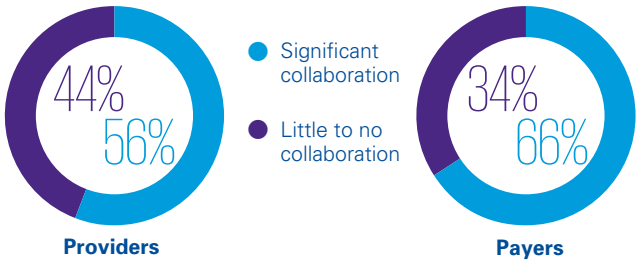
Payers

And yet, four out of ten surveyed organizations lack a formal program for managing connected device risks.



Formal programs for medical device risks

And, only a little more than half of surveyed providers and payers are collaborating with medical device manufacturers around device security.



Providers **Payers**

2017 KPMG/Forbes Insights Cyber-Security Survey

As shown in the chart at right, provider organizations rank medical device breaches toward the bottom of their security concerns, perhaps because they perceive that they have more urgent challenges to tackle. More than twice as many providers ranked malware as their top security concern as they did medical device security.

In our experience with clients, it has become clear that some hospitals are not fully aware of new risks that could arise from using interconnected medical devices without embedded security controls. For example:

- Even the most rudimentary internet-enabled device could be an entryway to a hospital's internal network.
- Patient information can be modified as it is transferred from a device, such as an infusion pump, via a web interface to an electronic medical record.
- Wireless radio waves in wearable devices, e.g., insulin pumps and continuous glucose monitors, present opportunities for hackers to execute *man-in-the-middle* attacks, i.e., interception of radio wave signals to alter device functionality.
- As an organization considers its medical device lifecycle management, it is important to remember that retrofitted devices may not provide sufficient protection.

According to David Remick, Partner, Life Sciences Leader, KPMG Cyber-Security Services: "The sophistication of cyber-attacks is snowballing on a daily basis. The only way organizations can stay ahead of malicious actors is to incorporate risk identification and mitigation at the earliest stages of medical device development. Manufacturers cannot do this alone. They need the insight and cooperation of their provider peers to really understand where attack vectors lie and how to keep patients safe."

In addition to collaborating with manufacturers to address cyber security and privacy from a technology perspective, providers need to address process and people issues. For example, they should upgrade their access management programs and establish clinician and patient education programs that cover the latest cyber-safety and privacy practices.

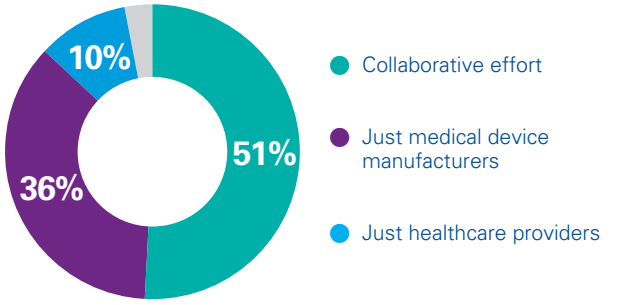
Provider Security Concerns

Malware	72%
HIPAA violations/compromise of patient privacy	55%
Internal vulnerabilities (employee theft/negligence)	47%
Aging IT hardware	40%
Shortage of qualified IT staff	38%
Out of date security software	35%
Medical device security	35%

2017 KPMG/Forbes Insights Cyber-Security Survey

The manufacturer's perspective

On the other side of the industry spectrum, medical device manufacturers seem to be moving more rapidly toward collaboration with healthcare providers. More than half of those surveyed believe that a collective effort with provider organizations is the key to securing medical devices.



2017 KPMG/Forbes Insights Cyber-Security Survey

And, they are taking action. Sixty percent of respondents indicated that their efforts include regular communication and coordination with providers, as well as patients and other device manufacturers.

It is critical that manufacturers steer away from considering cyber-security and privacy to be bolt-ons to development efforts. Instead, they should integrate them into device design from the earliest stages.

This can be done, for example, through state-of-the-art encryption, secure operating systems, and memory protections from malware. Of course, older devices were not originally designed with this level of security, although many have been retrofitted with some security capabilities.

There is some cause for hope going forward, as 92 percent of manufacturers surveyed by KPMG say they have integrated security and privacy principles into the development lifecycle of their devices. Further, 65 percent evaluate medical device security through penetration testing, 49 percent use bug bounty programs, and 48 percent undergo regular attestation testing.

While manufacturers are embracing the need to make cyber security and privacy part of device design, they must also ensure that technology modifications don't jeopardize device performance. It is of some concern that only 15 percent of manufacturers provide regular training to software engineers on secure development and programming practices. And 47 percent provide training as infrequently as quarterly or annually.

There is clearly room for improvement, perhaps by refining the range of players responsible for device security. While information security teams were responsible at 71 percent of organizations surveyed, product design held primary responsibility at only 57 percent.

Other actions manufacturers can take to help providers manage medical device cyber-security and privacy risks include:

- Aligning with industry competitors to develop universal security standards that can be used across the diversity of devices on the market.
- Adopting a principles-based point of view on privacy that better protects at-risk data assets.
- Coordinating with providers on an automated, efficient patch system protocol that meets the needs of both sides.

Conclusion

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 and the ability to treat patients rapidly in an emergency and improve their health outcomes over time. None of these objectives can be reached without collaboration and shared accountability.

Michael Ebert, Partner, KPMG Cyber-Security Services cautions: "Healthcare and life sciences are only now in the beginning phases of what is going to become one of the most data-intensive industries imaginable. They are, therefore, among the most susceptible to cyber risks. In light of these shifts, the industry as a whole needs to revisit its core processes and its willingness to collaborate on solutions – starting yesterday."

How KPMG can help

KPMG's Cyber Practice assists organizations from pre-breach to post-breach with an eye to transforming their security, privacy and business continuity controls into business-enabling platforms. Our philosophy is that security is a process and not a solution. Therefore, safeguarding IT networks and sensitive data from electronic attack and exposure is a constant endeavor.

Our teams have significant on-the-ground credentials in the cyber-security space, 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.

In particular, 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. Our incident response process is based on such internationally accepted frameworks as NIST SP800-86, ISO 18044:2004, and the SANS Six-Step IR Process. 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.

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

Contact us

Liam A. Walsh
Partner and Advisory Line of Business Leader, Healthcare & Life Sciences
312-665-3066
lawalsh@kpmg.com

Alison Little
Principal, U.S. Life Sciences Advisory Leader
973-912-4611
jalittle@kpmg.com

Michael Ebert
Partner and Cyber-Security Services Lead, Healthcare & Life Sciences
267-256-1686
mdebert@kpmg.com

David Remick
Partner and Life Sciences Lead, Cyber-Security Services
404-222-3138
jremick@kpmg.com

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

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

kpmg.com/socialmedia