The world of cyber risk continues to develop and expand since our May 2016 paper on Medical Device Cybersecurity. The threat of ransomware has come to the forefront as demonstrated by global attacks such as Wannacry and Petya. These attacks show how hackers have become more sophisticated in their ability to use malware to exploit vulnerabilities in systems, hardware, and devices, as well as highlighting the vulnerabilities of devices and systems that, through their lack of patching and support, and outdated operating systems, are exposed to hacking, worms, etc., that can affect patient safety, system security and data integrity.

The number of connected devices in the Internet of Things (IoT) continues to grow, both globally and within the healthcare industry, expanding the playing field for hackers. Many of those devices, even new ones, are not supported by the device manufacturer in terms of software security and updates. These vulnerable devices help to spread attacks quickly and efficiently.

At the same time, the healthcare industry’s reliance on connected devices continues to grow, as technology and efficiency drive progress. Regulatory oversight has built up steam, although no actual cyber security regulations have yet to be imposed upon the device manufacturers.

Our May 2016 paper considered the vulnerabilities of medical devices as well as examples of hacks that might cause bodily injury. We reviewed the then-current state of regulatory oversight, before considering the responsibilities and liabilities of the numerous implicated parties (from device manufacturer to healthcare provider to IT consultant) and the likely response from their various insurance policies (products, professional, recall, technology errors & omissions, cyber, kidnap & ransom to directors & officers liability policies).

We will review recent developments in cyber security threats as they relate to medical devices and the IoT. We will also review the progress towards formal regulatory oversight of medical device software and security, and the insurance industry’s response to this developing landscape.

Cyber Security Threats Related to Medical Devices (and the IoT)

Healthcare providers are increasingly connecting medical devices to their networks to provide up-to-the-minute information. This connectivity, wireless or not, exposes the devices to the same vulnerabilities as other connected computing devices. This includes the possibility that an intruder can gain access into the device, breach its security and spread a virus or malware, or access and collect data or alter the proper functioning of the device.

Connected medical devices of all types are vulnerable—including consumer devices, the associated mobile environment and implantable devices, from pedometers to bedside monitoring equipment to insulin pumps, pacemakers and biomarkers that measure medication adherence and geofencing the elderly. The more connectivity, the greater the risk posed — it is logically easier for an intruder to access a device if it is connected to the internet or a network.

The devices are typically connected to the internet directly or to providers’ networks, administrative and clinical IT systems and electronic medical records. The devices commonly run on standard operating systems and are often built on open infrastructure standards that hackers already attack in other computer equipment. Often, the devices do not run anti-virus software, are difficult to patch and still run factory-set passwords that can be found in standard device documentation.

Medical devices are one type of device in the Internet of Things (IoT), being the network of physical devices, vehicles, buildings and other items embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.

As the use of connected devices grows, so too does the potential for a security breach that impacts device functionality, patient safety, to other connected devices and all patient data. A survey released by Altman Vilandrie & Company in June 2017 reported that 46 percent of companies that buy IoT security admitted they had experienced an IoT-related intrusion or breach within the last two years. In many ways, medical devices are the weakest link in provider security systems, vulnerable as an access and launching point to the rest of the network.

Further, Ponemon Institute’s research report “Medical Device Security: An Industry Under Attack and Unprepared to Defend” reported in May 2017 that:

- 67 percent of reporting device manufacturers and 56 percent of healthcare delivery organizations think an attack will target a medical device used by or built by them in the next 12 months.
- 39 percent of device makers said that attackers have taken control of medical devices, and 38 percent of healthcare delivery organizations said that inappropriate therapy/treatment had been delivered to patients because of an insecure medical device.
- Only 17 percent of device makers and 15 percent of healthcare delivery organizations confirm that they are taking significant steps to prevent attacks.

---

1 Gallagher Healthcare Practice “Medical Device Cybersecurity” [https://www.aig.com/knowledge-center/whitepapers/medical-device-cybersecurity/]
The issue is not just one of patient safety, but also of the integrity and security of systems in general. Additionally, medical devices have often been purchased by departments other than the IT department, thereby becoming endpoints that have not been vetted and maintained by IT.

The Wannacry ransomware attack in May 2017, which targeted computers running unpatched Windows OS through a network worm, affected businesses around the world and even caused the United Kingdom's National Health Services to run some services on an emergency-only basis, which affected not just computers themselves but also devices such as MRI scanners, blood-storage refrigerators and theater equipment.

Instances of actual patient harm remain rare, but device vulnerabilities have come to light. For example, on January 9, 2017, the U.S. Food and Drug Administration (FDA) issued a Safety Communication confirming vulnerabilities in St. Jude Medical’s implantable cardiac devices and Merlin@Home Transmitter that could allow unauthorized users to remotely access, control, and issue commands to compromised devices. St. Jude has since developed a software patch to fix the vulnerabilities.

**Regulatory Oversight of Medical Device Software and Security**

The FDA is responsible for protecting and promoting public health through the control and supervision of, among other items, medical devices. This includes medical applications that are medical devices and whose functionality could pose a risk to a patient’s safety if the mobile app did not function as intended.

This guidance is in the form of nonbinding recommendations providing direction to device manufacturers on how to monitor, identify and address cyber security vulnerabilities, as well as identifying which device modifications that address cyber security vulnerabilities should be reported to the FDA by manufacturers. This guidance follows the FDA’s 2014 recommendations to consider cyber security during the design and software validation process for devices.9

The FDA is increasing the scrutiny on device manufacturers to address cyber security risk when the device is first being designed, and throughout its lifecycle. The premarket considerations should include:

- Identification of assets, threats, and vulnerabilities;
- Assessment of the impact of threats and vulnerabilities on device functionality and users/patients;
- Assessment of the likelihood of a threat and vulnerability being exploited;
- Determination of risk levels and suitable mitigation strategies; and
- Assessment of residual risk and risk acceptance criteria.

Postmarket, the FDA recommends a risk management program to address vulnerabilities that may result in patient harm, including:

- Monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk;

---

7 FDA Safety Communication https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm555843.htm
• Maintaining robust software lifecycle processes that include mechanisms for monitoring third-party software components for new vulnerabilities throughout the device’s total product lifecycle and for design verification and validation for software updates and patches that are used to remediate vulnerabilities, including those related to off-the-shelf software;

• Understanding, assessing and detecting the presence and impact of a vulnerability;

• Establishing and communicating processes for vulnerability intake and handling;

• Using threat modeling to clearly define how to maintain safety and essential performance of a device by developing mitigations that protect, respond and recover from the cybersecurity risk;

• Adopting a coordinated vulnerability disclosure policy and practice; and

• Deploying mitigations that address cybersecurity risk early and prior to exploitation.

Additionally, the FDA has taken care to emphasize that cybersecurity risk management is a shared responsibility among all stakeholders, including the medical device manufacturer, the user, the IT system integrator, health IT developers and an array of IT vendors that provide products that are not regulated by the FDA. This reflects the analysis in our May 2016 paper that considered the responsibilities and liabilities of the numerous involved parties, and the likely response from their various insurance policies (from products, professional, recall, technology errors & omissions, cyber, kidnap & ransom to directors & officers insurances).

Further, the FDA is proceeding with its planned National Evaluation System for Health Technology (NEST)\(^\text{10}\) which will integrate data from clinical registries, electronic health records, and medical billing claims to gather more comprehensive evidence of medical device safety and effectiveness.

In a parallel development, the Department of Health and Human Services’ Office of the Inspector General (OIG) issued an early alert\(^\text{11}\) on September 30, 2016, to the Centers for Medicare & Medicaid Services (CMS) encouraging CMS to include device identifier codes in its claims forms to assist with OIG’s tracking of devices, which are recalled or fail prematurely, to help ensure patient safety (as well as to identify costs).

California Senate Bill 327,\(^\text{12}\) introduced in April 2017, sought to require web-connected device manufacturers to equip devices with reasonable security features appropriate to the device and the information collected. The bill is currently inactive, but indicates interest at the state legislature level in holding device manufacturers more accountable for data security.

The Health Care Industry Cybersecurity Task Force, established by the Department of Health and Human Services, issued a report in June 2017\(^\text{13}\) on methods to improve cybersecurity in the healthcare industry, and made a number of recommendations on medical device cybersecurity, including:

• Secure legacy systems through creating an inventory; replace/upgrade where possible; document retirement timelines; and make updates and patches;

• Improve transparency between developers and users, including a clear description of components and risks;

• Implement security by design throughout the product lifecycle;

• Require strong authentication, pending a national standard, and adopt National Institute of Standards and Technology (NIST) guidelines for remote access; and

• Establish a Medical Computer Emergency Readiness Team to coordinate responses to incidents.

In June 2017, the Federal Trade Commission (FTC) submitted public comments\(^\text{14}\) to a working group convened by the U.S. Commerce Department’s National Telecommunications and Information Administration (NTIA) that is developing guidance about ways for IoT device manufacturers to better inform consumers about security updates related to the devices. Those comments included suggestions that manufacturers should consider conveying to consumers information as to whether the device can receive security updates, how it will receive them, and when support for the device would end. Further, the FTC

---

10 FDA website https://www.fda.gov/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/ucm301912.htm
11 OIG alert https://oig.hhs.gov/oas/reports/region1/11600510.asp
12 California Legislative Information http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327
suggested that device manufacturers should consider using a uniform notification method to inform consumers about security updates, and allow consumers to sign up for notifications about security support.

On August 1, 2017, a bipartisan group of Senators introduced the Internet of Things (IoT) Cybersecurity Improvement Act of 2017 to improve the cyber security of internet-connected devices that are purchased by the U.S. government. The proposed minimum standards include requirements that devices be patchable and do not include passwords that cannot be changed.

**Insurance and the Developing Threat Landscape**

Our May 2016 paper considered how security vulnerabilities in medical devices leave devices and their users/owners open to illegal and intentional activity, whether targeted or not, which can impact the security of patient data, the safety of patient care and the successful operation of the healthcare business. Patients will hold their healthcare provider responsible for security breaches in devices that are recommended or used by their physicians. The consequences to the provider of security breaches include liability for financial loss and bodily injury, their own business interruption and damage to reputation.

Insurance coverage for this exposure can be found under many different coverages, from the provider’s cyber, medical professional liability, general liability and property insurances to the IT vendor’s errors & omissions liability insurance to the device manufacturer’s product liability, professional liability and product recall insurances.

Recent threat and incidents, such as Wannacry, Petya and continuing targeted ransomware demands, have affected healthcare organizations at the system security level and in terms of patient safety. These threats have brought greater emphasis to the value of the various insuring agreements of a typical cyber policy. In particular, these threats have the potential to trigger many of a cyber insurance policy’s insuring clauses as a result of a single incident.

For example, a worm, spreading a ransomware demand by means of the medical device, might now require the cyber extortion coverage to provide forensic advice and payment of ransom; the breach response coverage to address legal, forensics, notification and credit monitoring costs; the regulatory coverage to address fines and penalties; the liability coverages to cover claims from patients; the business interruption insuring clause to address lost revenue/profit; and the data restoration insuring clause to assist in recovering lost assets. Some policies include sublimits to address PR costs and reputational harm as well.

All this breadth of coverage can exist in a single policy (the provider’s cyber policy), making it imperative that provider insureds review their current policy limit to ensure that it is reasonably likely to address all of these different types of potential losses to the organization.

Overall, the threats are developing faster than the solutions. Vulnerabilities exist in many current medical devices, some of which can be addressed by changing passwords and patching, but some of which cannot be remedied without replacement. It is important that providers inventory their medical devices, understand the level of security (and risk) in each and plan accordingly. Just as the FDA balances risk against security in assessing products and devices, providers need to do the same. Some providers have already implemented procedures to assess cybersecurity risk in new medical devices, and address vulnerabilities accordingly. On the other hand, Ponemon Institute’s research report “Medical Device Security: An Industry Under Attack and Unprepared to Defend” found that only 35 percent of healthcare delivery organizations encrypt traffic among IoT devices, and 53 percent do not test their devices for vulnerabilities. Providers taking action in this area should explain to their cyber insurer that they are taking these proactive steps to improve the risk.

With regard to claims alleging bodily injury, we have seen some examples of the same insurer covering hospital professional liability and cyber (liability) insurances, aiming to avoid a gap between coverages for bodily injury. This practice is not widespread at this time.

Along similar lines, we see insurers of physician medical professional liability adding cyber coverage by endorsement. This can help avoid finger-pointing between insurers, but does not necessarily provide cyber insurance without a bodily injury exclusion, since these endorsements are often a pass-through to an established cyber insurer and the endorsements often exclude bodily injury either by way of a broad (arising out of, etc.) exclusion or, more preferably, a “for” exclusion. Some exclusions do contain carve-backs solely for mental anguish and emotional distress.

Other insurers are seeking broad answers to the question of bodily injury (and property damage) in relation to the failure of computer security. For example, a leading insurer expanded their cyber offering to address bodily injury arising out of the failure of a computer system (to prevent unauthorized access/use, denial of service attack or receipt or transmission of a malicious code) in the context of completed products and general liability insurances. Such coverage operates as excess, or difference in conditions, over the insured’s products and general liability policies.

---

Gallagher Healthcare Practice Medical Device Cybersecurity
Lastly, the issue of bodily injury arising out of cyber-attack or computer system failure is just another element in insurers' (and reinsurers') efforts to underwrite cyber risks that are based on a general lack of loss history (e.g., no broad experience of patient injury from cyber-attack) and which also have the potential to affect many insureds and their policies (an aggregation exposure that is also without meaningful loss history). Cyber risk is still in its infancy, and the insurance sector’s collective response will develop as claims and losses clarify liability and costs, and coverages develop to best suit the exposures.

Conclusion
It is still not clear who is ultimately, legally responsible for the cybersecurity of medical devices, but it is likely that all major parties, from the manufacturers to the healthcare providers to patients, have risk and must work together to safeguard medical devices. Indeed, while Ponemon Institute’s research report “Medical Device Security: An Industry Under Attack and Unprepared to Defend” found that 41 percent of healthcare delivery organizations believe they are primarily responsible for the security of medical devices, almost one-third of both device makers and healthcare delivery organizations say no one person or function is primarily responsible.

Insurance remains valuable to all the stakeholders, through the transfer of not only the risk of certain events causing loss or liability, but also the additional legal risk of being responsible for the ultimate responsibility for patient harm.

We have seen that although some medical device manufacturers and healthcare providers are taking significant steps to prevent cyber attacks, there is already a large, established base of medical devices that are not secure and will mostly remain unsecured for the remainder of their usable lives. New devices will increasingly be designed and supported to be secure and patched, and regulations will eventually force all parties to new standards but, nevertheless, there is a real exposure that needs to be addressed now.

Providers must ensure that their insurance coverage will respond to these developing threats. This will involve a detailed understanding of healthcare, the provider’s business, its contracts and insurance policies, as well as which insurances should be required of vendors such as consultants and the medical device manufacturers themselves.

Risk managers should work with their advisors to review the developing policy coverage options, understand how the various coverages will apply in the event of a breach of cybersecurity of medical devices and determine how the policies fit together and the order in which they will respond. From this process, risk managers and their advisors will be able to find the gaps, press insurers to tailor their coverage offerings accordingly and require vendors to maintain the appropriate coverage.

Additionally, risk managers can mitigate their medical device security risk through promoting an inventory of devices and their security; replacement of unsecured devices at the earliest opportunity; education of the senior management of these risks and their impact on insurance decisions and costs; and pressure on IT procurement to purchase (more) secure devices that are designed with security in mind and that are better supported and patched through their lifecycle.
About the Author

Trevor Weyland is an Area Senior Vice President in Arthur J. Gallagher & Co., specializing in executive and management liability issues with cyber expertise for Gallagher’s Healthcare Practice. This practice focuses on providing insurance and risk management solutions to meet the unique needs of healthcare providers and facilities across the continuum of care.

For more information, contact:

Trevor Weyland
Gallagher Healthcare Practice
trevor_weyland@ajg.com
818.539.1224

www.ajg.com/healthcare
www.ajg.com/cyber
www.ajg.com/mlp