

Safety Newsletter

Cyber Security

April 2024

Even as healthcare organizations are partnering to innovate and explore new technological advancements, harness AI, leverage health management and monitoring technologies, and utilize medical devices, the recent cyber-attacks of Change Healthcare, a revenue cycle system used by many hospitals, and Lurie Children's Hospital in Chicago, sheds a bright light that cybersecurity concerns have not lifted.

Marsh McLennan Agency has professionals to help your organization sift through your potential risks and determine the most appropriate coverages, including those for cybersecurity. Additionally, we have a [Cyber Resiliency Network \(CRN\)](#) to help make it easier to access unparalleled cyber resources so you can tackle novel, emerging challenges as they arise. Our CRN offers vetted partner resources to assist you with three distinct areas of cyber risk management: information security, legislative compliance, and organizational education.

As an MMA client, you receive exclusive access to a number of complimentary or discounted services from our partner network. This opportunity affords you and your organization critical resources that could save you from digital devastation, regardless of your organization's current cybersecurity infrastructure.

This month we also wanted to share a recent excerpt from *The Council of Insurance Agents & Brokers Leader's Edge Magazine* that describes some new regulations the FDA is rolling out related to cybersecurity and medical devices. Following this Q&A are some frequently recommended steps that you can take should you suspect or determine an unauthorized access or use of your computer network.

Cyber Guidelines Target Medical Devices

Q&A with Matthew Zagwoski, Product Leader in Global Life Sciences, Beazley Group

Q: Why has the FDA released this new iteration of its cybersecurity regulations?

The FDA really started putting guidance out for the industry—in terms of how to manage cybersecurity threats when you have devices that are connected to the internet—back in the early 2000s. But in recent years, cybersecurity issues have become more in the forefront because, every day, there's an attack on a healthcare provider who had to shut down. So, the FDA asked for an FBI review of a number of industries, and specifically healthcare, to assess cybersecurity vulnerabilities.

A: What came out of that was an understanding of healthcare institutions and how they're integrating technology, using all of these connected devices, and then looking at the threat vectors. This created the realization that, while we



Marsh McLennan Agency Risk Control Contacts

RiskControlNW@MarshMMA.com

Brodie Loushin | (406) 533-1038
Pat McCarthy | (406) 327-6519
Shawn McDevitt | (406) 533-1016
Randy Mcleod | (509) 907-7268
Brendan Riley | (406) 457-2114
Rob Wynegar | (406) 268-2591

MMANorthwest.com

have great regulations in terms of the safety and the efficacy of medical devices, we really don't have anything hardwired in place that the FDA can look at and say, "Alright, now we know they're cybersecurity." That's becoming a much bigger issue now. With the analysis that the FBI did, it's easy to see that anybody can hack into this stuff and potentially cause harm—reprogram a pacemaker, change some settings on a radiology machine. All the IV drips run through these new wireless devices so they can be controlled from the nurses' station. If someone can get in and change these settings to cause harm, either directly to the patient or from a terrorist standpoint, that is a pretty big risk.

Q: What do these new requirements do to help ensure medical device manufacturers create products that are more cybersecurity?

A: Through the Consolidated Appropriations Act of 2023, they put a new section into the Food and Drug Consumer Protection Act addressing this vulnerability. One could say that it's been a long time coming in terms of addressing some of these vulnerabilities, but I think the time is right for it. That's what spawned this whole new evolution, which gives the FDA more power in terms of making sure that the devices that are out there are actually secured and will remain secure throughout their life cycle. The FDA said, as of Oct. 1, if you want to release any new device on the market that is wireless or has a way of connecting to the internet to transfer data, you have to "reasonably assure" us that the device is cybersecurity. That's a subjective comment, "reasonably assure." But the FDA has an 80-page list of all these things manufacturers should endeavor to do to assure them [the FDA] that a device will not only be cybersecurity but they can patch it and maintain it after it's been put in place. Companies have to track it, assess it and patch it through the life cycle of the entire device.

Q: I would think this could mean a lot of money that device manufacturers will have to spend on cybersecurity, correct?

A: Yes. If I'm a company making an insulin pump, my focus is always on making a better insulin pump—one that does everything better than my competitor. But I'm not necessarily focused on it being the most cybersecurity insulin pump in the marketplace. So I'm not putting as much effort behind that part of it as I probably should. But now the FDA can refuse to accept any device that they claim is not cybersecurity.

Q: That will cause a lot of companies to take a step back and say, "I'm developing these things, but how do I make sure I have a product that is sellable before I put \$100 million into development? How do I make that money work the right way?"

A: A lot of the time you have to look at redesigning your whole development plan for that. Some companies might be so small they may have one person who understands, like their IT guy, but they don't necessarily have a troop of cybersecurity experts that understand it. I read something that said between 2020 and 2025 the average cost of cybersecurity will go up 15% on average, for the entire world, every year. In certain industries like healthcare, I can see that being a lot more.

Q: What kind of impact could that have on costs in the rest of the market?

A: I don't think companies are going to eat that money. I also don't think it's going to stand out enough that you can say your healthcare costs went up X percent because of this regulation. I think it will just be swept up in the totality of it all. We're in an inflationary market right now, and I still talk to clients who struggle to get the raw materials they need to make their products. That has had an indirect cost on everything. This is just one aspect of a multitude of things that's just going to keep feeding that machine, unfortunately. One could hope that making the switch now costs a bit more but that, down the line, it should balance out because we're not seeing as many hacks or issues we otherwise would have.

Q: If these changes are on devices coming to the market now, could healthcare organizations choose to keep ones they have and not incur some of the costs of newer devices?

A: I think that's going to be interesting to see how that plays out. In the new appropriations act, there was nothing that deals with the existing devices that are already in the market. There wasn't a time frame to phase out old devices. So, if I'm a healthcare institution, do I spend the tens of millions of dollars to update all of these things that I already have if I don't have to? But then if I don't update and am hacked, there's going to be a cost that comes from that. If a hospital did have a big event and people were injured, someone could say the hospital specifically kept devices that were not as maintained as the new regulations, so they created an environment that caused someone bodily injury. And then they could sue in civil court for that.

Information provided by Leader's Edge.com

Developing a Cyber Incident Response Road Map

The following are frequently recommended steps upon suspected or determined unauthorized access or use of your computer network. This includes potential theft, loss, or unauthorized access/use of sensitive, personally identifiable information or third-party corporate information in your care, custody, or control.

A successful response involves prompt coordination of resources, and the actions below can help business leaders plan ahead and strengthen their response and recovery efforts.

1. Recognize the potential or confirmed cyber incident.

Mobilize your internal incident response team to gather facts to establish what happened and when it was discovered. This includes finding which systems and devices are affected and what kind of data may be impacted.

2. Notify external partners (e.g., broker, carrier, or outside counsel).

With the developing facts, contact MMA to assist in helping you notify the affected parties. Each situation is unique and can occur at all hours of the day. You may want to consider directly notifying your cyber carrier immediately using the 24/7 hotline or email.

Be mindful of utilizing electronic communications such as email if a suspected system compromise is suspected. Avoid sending copies of your policy internally or externally.

Contact a member of your carrier's pre-approved privacy counsel with a focus on carrier consent and attorney-client privilege throughout the investigation. Coverage can be impacted if vendors are not pre-approved by the carrier and most have panel vendor requirements.

3. Seek forensics assistance if necessary.

Counsel will assist you in determining whether an external forensic firm will be needed to support your internal investigation. This will likely require approval by your carrier of the specific scope of work necessary to determine the existence, cause, and impact of the incident. This is because the data involved in the incident that will be reviewed is likely highly sensitive.

4. Conduct initial scoping calls and foster carrier involvement.

Consistent communications with the carrier representative establishes a good working relationship. Keep lines of communication open and foster collaborative investigation and response efforts. Common topics such as pre-approval of the specific forensics scope of work necessary for the investigation and self-insured retention erosion should be a top priority. MMA will continue to support you throughout the process.

5. Other vendor considerations.

In the event security breach notice law(s) require direct compliance including notification to individuals or regulatory agencies, additional vendors may be needed to support the process and carriers often require pre-consent for vendors and public relations/crisis communication firms.

It is strongly recommended you use carrier approved incident response firms to help streamline the process and to minimize the chance of having expenses that are not covered by your policy.