CONNER STRONG & BUCKELEW

HIDDEN CYBER SECURITY RISKS IN CLINICAL TRIALS

Why Patient Safety, Personal Information, and Sponsor IP is at Risk

Digital health capabilities are revolutionizing the way individuals receive healthcare. But in today's network-connected world where data breaches and cybersecurity events are growing in frequency, the rise of digital capabilities introduces an evolving cyber risk to clinical trials that may be addressed with insurance coverage and cutting-edge protections.

Digital health encompasses wearable devices, the digitization of medical records, video conferencing between patient and doctor and drives multiple facets of a clinical trial. Digital health is being introduced to nearly every corner of the healthcare market as well.

Outside investors have sunk **more than $20 billion**[1] into the development of digital health capabilities over the past three years, and experts expect this number to **continue to climb** as new applications come to light.

These capabilities are improving the accuracy and speed in which doctors can diagnose, manage, predict and prevent medical issues. They're extending medical services to rural areas where access to treatments is sparse. Digitizing medical records provides doctors and healthcare professionals with fast access to more information they can analyze and use to make better medical decisions and recommendations.

[1] https://www.accenture.com/t20171108T183552Z__w__/us-en/_acnmedia/PDF-57/Accenture-Health-Digital-Health-Comes-Of-Age.pdf

CONNER STRONG & BUCKELEW

CONNER STRONG & BUCKELEW

Digital health encompasses wearable devices, the digitization of medical records, video conferencing between patient and doctor and drives multiple facets of a clinical trial. Digital health is being introduced to nearly every corner of the healthcare market as well.

Consulting firm Accenture predicts that approximately **25 million individuals**[2], or one in every 13 patients, **will have their medical or personal information compromised** via a breach of their healthcare provider's digitized records by the end of 2019.

Data breaches aren't the only cyber threat facing the medical industry. Ransomware attacks, in which cyber criminals hold a network or database hostage in exchange for payment, have skyrocketed in recent years. Cyber criminals are even capable of hacking into a medical device currently being worn by an individual, putting patient safety at risk.

Digital innovation also introduces cyber risks to clinical trials, which are markedly exposed given the wide range of parties involved as well as the wealth of information being stored throughout the process. These risks affect the entire cast of participants. The trial sponsor, the investigators, clinical research organizations (CROs) and even human subject participants are exposed to cyber security threats.

The push for innovation through the adoption of digital health in clinical trials will not slow down anytime soon. Clinical trial players must start by identifying their risks and responsibilities. From there, those involved must decide which risks to manage themselves, and which to transfer through the use of insurance coverage.

[2] https://www.accenture.com/t20171221T005341Z__w__/us-en/_acnmedia/PDF-54/Accenture-Health-Cybersecurity-300-Billion-at-Risk.pdf#zoom=50

CYBER RISKS IN CLINICAL TRIALS

Digital health capabilities introduce new cyber risks to the entire cast of participants in a given clinical trial. The digitization of health records puts trial participants' healthcare information at risk as data breaches become more commonplace across the industry. These individuals can also face physical dangers if a wearable administering treatment is compromised while in use.

For trial sponsors, the valuable intellectual property obtained throughout the trial is also at risk of being compromised in a data breach. One overlooked potential consequence from a cyber-attack are files and documents that are damaged, contaminated, deleted or held for ransom by cyber criminals. The financial impact can cascade from losing the up-front costs of a trial to investing further resources to redo a trial, even when future commercialization remains uncertain. For trial sponsors that have invested millions into a clinical trial and have much to gain from obtaining regulatory approval, losing this intellectual property, or the ability to use the data, can be devastating.

Sponsors, investigators and CROs can also be held liable for the heavy financial and reputational damages that may result from a large-scale breach of patients' personally identifiable information.

> Suffering a data breach can cost a company $3.8 million per incident[3] after factoring in a robust response plan, offering credit monitoring to all affected and other ancillary costs.

This, however, does not capture the reputational damage that can result from being associated with a cyber event. According to an Accenture analysis, healthcare providers that do not make cyber security a strategic priority will put $305 billion of cumulative lifetime patient revenue[4] at risk over the next five years.

It is clear to see why cyber criminals are targeting the healthcare industry. Medical records contain extremely sensitive personal information, which can sell on the dark web for as much as 10 or even 20 times[5] more than a Social Security number or a credit card number.

As sponsors, CROs, investigators and everyone else involved in a clinical trial continue to lean more heavily on digital tools to conduct trials, they must verse themselves with the intricacies of these risks and make cybersecurity a strategic priority. Clearly, all parties involved in clinical trials must pay close attention to the growing threat of a cyber-attack.

[3] https://www.ibm.com/security/data-breach

[4] https://www.accenture.com/t20171221T005341Z__w__/us-en/_acnmedia/PDF-54/Accenture-Health-Cybersecurity-300-Billion-at-Risk.pdf#zoom=50

[5] https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924

CONNER STRONG & BUCKELEW

CYBER INSURANCE'S CRITICAL ROLE

Insurance plays a pivotal role in protecting sponsors, CROs and investigators from losses resulting from a cyber-attack. Product liability, bodily injury, property, errors and omissions liability, directors and officers liability, business interruption and cyber coverage are all key aspects of a well-rounded insurance package that can offer financial protection from the fallout of a cyber security event. This is clearly illustrated by the impact to Merck resulting from the June 2017 "NotPetya" cyber-attack which threatened the production and supply of life-saving drugs like Keytruda for cancer, Januvia for diabetes and Zepatier for treatment of hepatitis C. In such cases the potential business income loss resulting from property damage or non-damage scenarios along with reputational injury may prove fatal to clinical stage companies.

Aside from the well-documented damages associated with a data breach, the utilization of network-connected wearable medical devices introduces the risk of bodily injury should a device be hacked while being utilized by a trial participant.

For instance, a network-connected pacemaker that is hacked and manipulated by a cybercriminal while in use could lead to devastating injury or even death.

While product liability policies have not contained exclusions for cyber events, there have been recent examples of insurance companies attempting to add such endorsements to "clarify coverage." In some cases, the endorsements may exclude cyber and then give back bodily injury, property damage or ensuing financial loss, but only if reasonable precautions can be met. Since approval of a medical product by the FDA incorporates what it decided are "reasonable precautions," it is possible that such insurance demands may not be consistent with that approval, creating a dangerous point of potential conflict in the event of a claim. Since product liability is an essential coverage, it is important to work with your insurance agent or broker to assure that the coverage remains free of such pitfalls.

CONNER STRONG & BUCKELEW

These lessons demonstrate that there are a variety of evolving risks which must be addressed with a robust mix of insurance coverage, including product liability, clinical trials, personal injury coverage and both first- and third-party cyber policies. Since cyber negligence from suppliers may lead to disputes and ultimately subrogation and recovery demands that add tension to often essential relationships, it is important to include language in contractual agreements with third-party vendors that clearly define liability and employment of reasonable risk management precautions in the event of a cybersecurity breach. Finally, it is important to select an insurer who can provide reputational damage coverage and access to experts to help manage the potential disruptions arising from a cyber-attack.

> Cyber insurance, while still somewhat overlooked by many life sciences companies conducting clinical trials, is an absolutely critical component in protecting a company from the impact of a cybersecurity event.

These policies are easily triggered and typically cover most, if not all, expenses related to a cyber security event, depending on the policy. Financial damage resulting from malware, ransomware, corrupted data attacks, etc. may be covered by a typical cyber policy without much need for amending policy language or negotiating exclusions.

These coverages also come with pre- and post-event mitigation services that can go a long way in preventing a breach from occurring and limiting the damage after one takes place. Cyber insurance allows policyholders to tap into the underwriters' network of vendors that specialize in data breach forensics, response plans, public relations and loss mitigation services. Without a policy, life sciences companies would be on the hook for all of these expenses, as well as any credit monitoring services, business interruptions and customer outreach that may be necessary after an attack.

Pricing for this coverage varies widely based on an organization's size and specific needs. But the leading underwriters with whom we speak in the insurance industry suggest that a company's ability to demonstrate its resiliency to a cyber-attack can drastically impact cyber policy pricing. For instance, a trial sponsor that has a robust response plan in place, practices it regularly and trains its employees on a monthly basis about the latest phishing techniques will pay considerably less for the same coverage than one with limited cyber security precautions in place.

CONNER STRONG & BUCKELEW

BENEFITS OF DIGITIZATION

While there are risks involved, clinical trials are undeniably benefitting from digitization in powerful ways. For example, wearables can monitor a participant's medical condition remotely throughout the course of a clinical trial with astonishing accuracy. These wearables are leading to the growth of both the quantity and quality of information produced throughout a trial. Electronically storing this information makes data analysis faster and more effective than ever before.

In fact, an increasing number of decentralized clinical trials are reducing the number of on-site visits a patient is required to attend and can collect data remotely from a patient's home. I spoke to Michael O'Brien, a senior clinical research executive who has spent the last five years commercializing and promoting the benefits of decentralized trials. Through the use of wearables, video conferencing and the digital transmission of readings and data, trial sponsors that engage in these clinical trials are able to reap a number of benefits.

> By eliminating the need for participants to travel and spend time at a clinical trial site, sponsors are able to vastly increase the reach of their recruitment efforts.

With reduced geographical barriers, sponsors can realize a higher availability of participants from across the country who meet the study's needs. Wearable medical devices monitor patient health information, and participants are directed to administer study drugs from their own homes. Additionally, video and data network connections can ensure that medical readings are precisely recorded, time stamped and immediately organized to limit the potential for human error.

"In reducing the burden on patients by transferring clinical research activities to the home, sponsors can increase the reach of their participant recruitment efforts, eliminate overhead costs and increase the speed, quantity and quality of clinical trial data," O'Brien told me in an interview.

> "With the increasing pressure on drug pricing and elevated costs of drug development, digitally enabled approaches such as decentralized trials can contribute meaningfully to a more efficient drug development process."

These decentralized clinical trials encompass nearly the full spectrum of digital health capabilities and have the potential to revolutionize the way clinical trials are conducted. Clearly, they offer a unique and powerful step forward in the evolution of clinical trials.

Such trials also introduce a few more areas of potential security vulnerability. For instance, personally identifiable information and the intellectual property of the sponsors must be transmitted wirelessly from a participant's home network, which may not contain a robust cybersecurity system. This network may serve as a weak link hackers can use as avenue to exploit. Patching up this potential security weakness will require sponsors, CROs and subjects to work together to ensure the security of all participants is maintained.

While the prospect of decentralized clinical trials is a compelling concept, the fact remains that the majority of trials continue to involve more traditional sites and data collection methods. But even these formats are still markedly exposed to cyber security risks. In fact, whenever network-connected devices and equipment are introduced to a process, cybersecurity vulnerabilities inevitably also arise. While these risks can be managed, it is important for clinical trial sponsors, CROs, investigators and everyone else involved to understand where they stem from and what exactly is at stake.

GRAY AREAS OF LIABILITY

Digital health introduces new technology providers, third-party data maintenance and storage vendors, software developers and a litany of other parties to the clinical trial process. Given this wide cast of participants, all with varying degrees of exposure and responsibility to sensitive information and network-connected equipment, establishing liability after a cybersecurity event can be difficult.

For instance, the creation of a wearable device involves countless parties, including developers, manufacturers, installation services and maintenance professionals. Flaws or errors and omissions in the design, manufacturing, implementation or maintenance of these devices may leave behind software bugs or programming faults that can be exploited to alter treatment or the data a sponsor counts on to achieve regulatory approval.

> If a wearable device is compromised and it leads to an individual being hurt or other costly consequences, determining which of these parties is liable to damages can be a difficult task.

This gray area of liability is another evolving aspect of cybersecurity worth monitoring. As technology and digital capabilities evolve, the standards for establishing liability are likely to change. This fact further underscores the need for a robust insurance package to ensure each organization is protected from liabilities they may not even be aware of. With so many different parties involved, it is essential that clinical trial insurance packages include blanket contractual coverage that protects the organization from damages caused by third-party vendors. These companies must also require that vendors name them as additional insureds in their contracts to protect the sponsor's interests in the event of a cybersecurity breach.

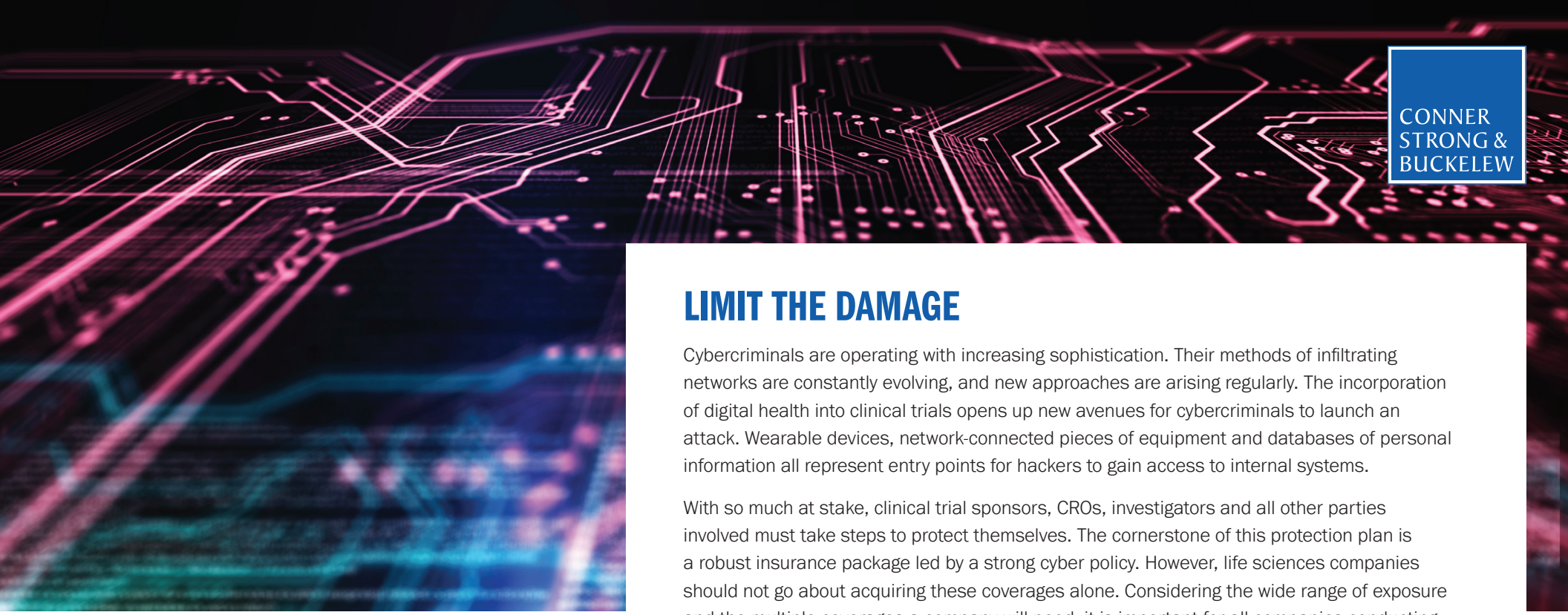
HEIGHTENED REGULATORY AND LEGAL RISK

Regulators and lawmakers are also taking notice to the rise of cyber security events in clinical trials and the broader healthcare industry. As a trial sponsor, investigator or CRO, there's a lot to keep track of from a legal and regulatory perspective.

In 2018, the FDA issued a playbook[6] to address continued threats to medical devices that could affect client safety, including cybersecurity. The playbook looks at medical devices as it pertains to their design labeling and documentation of risk. HIPPA and HITECH have long been around to protect the personal information of patients, but are perhaps more relevant today than ever before given these new cyber liabilities. According to James Bird, Executive Director Life Sciences and Healthcare with Price Forbes & Partners Ltd in London, the U.S. is far from the only country taking notice. The European Union recently enacted General Data Protection Regulation (GDPR) to further protect the personal information of citizens. Fines and penalties are insurable where allowed by law. Unfortunately, GDPR will contain a mixture of jurisdictions, most not allowing this response.

Cybersecurity and the protection of personal information has become a global issue that is attracting the attention of a wide range of governing bodies. With so many different regulators and lawmakers taking a close look at the issue, it has become difficult for trial sponsors, CROs and investigators to discern their own legal and regulatory liabilities and obligations within the context of a clinical trial. The evolving legal and regulatory landscape as it pertains to cyber security and digital innovation in healthcare is certainly worth monitoring.

[6] https://healthitsecurity.com/news/fda-unveils-mitres-medical-device-security-playbook



CONNER STRONG & BUCKELEW

LIMIT THE DAMAGE

Cybercriminals are operating with increasing sophistication. Their methods of infiltrating networks are constantly evolving, and new approaches are arising regularly. The incorporation of digital health into clinical trials opens up new avenues for cybercriminals to launch an attack. Wearable devices, network-connected pieces of equipment and databases of personal information all represent entry points for hackers to gain access to internal systems.

With so much at stake, clinical trial sponsors, CROs, investigators and all other parties involved must take steps to protect themselves. The cornerstone of this protection plan is a robust insurance package led by a strong cyber policy. However, life sciences companies should not go about acquiring these coverages alone. Considering the wide range of exposure and the multiple coverages a company will need, it is important for all companies conducting clinical trials to consult an insurance broker that is well-versed in these policy intricacies before securing coverage.

While there is no surefire way to stop a cyberattack, cyber insurance is a necessary component to mitigating risk and managing the liability.

To learn more about Conner Strong's Life Sciences practice, visit:

CONNERSTRONG.COM

DAN BRETTLER

Managing Director, Life Science and Technology Co-Practice Leader

973 659 6456

dbrettler@connerstrong.com