Journal of Clinical Research Best Practices

Vol. 17, No. 8, August 2021 "Happy Trials to You"

Supply Chain Cybersecurity in Clinical Research

By Rebecca Rakoski

Supply chain cybersecurity became headline news when hackers planted malicious code in SolarWinds's IT management tool, Orion, and compromised the data security of thousands of its business customers and millions of their customers.[1] After all, why attack 100 different organizations, each with its own security system, when one-stop shopping is available from a single soft target?

Healthcare is a favorite target of hackers because of the time-critical nature of healthcare, the sensitivity of patient information, and the high value of intellectual property. For example, Doctors Medical Center of Modesto discovered that a contractor used by a former vendor accidentally exposed patient data over the internet for more than a year.[2] At least 21 hospitals suffered data breach through their vendor, CaptureRx, which helps Medicare and Medicaid patients access reduced prices on drug prescriptions.[3] A ransomware attack on eResearchTechnology, "a global data and technology company that helps minimize risk in clinical trials," directly affected several of its clients, including at least one company running Covid-19 vaccine trials.[4]

The Ponemon Institute recently published a report, "A Crisis in Third-party Remote Access Security."[5] According to the report, of organizations surveyed that had experienced a security breach within the previous 12 months, 74 percent attributed the breach to giving too much privileged access to third parties. More than half of the survey respondents said they were not assessing the security and privacy practices of all third parties before granting them access to sensitive and confidential information.

A typical clinical trial protocol can list a dozen solution providers, not even counting the study sponsor's and clinical research sites' numerous other solution providers. These solution providers all have their own vendors, and so on.

Despite these clear warnings, clinical research supply chain cybersecurity is far from robust.

Managing Supply Chain Cybersecurity Risks

From a practical standpoint, supply chain cybersecurity is only one of many risks that an organization must manage, to say nothing of all its other obligations and priorities. Complete protection is probably impossible without imposing security measures that make operations impractical. The issue is thus not eliminating risks but minimizing them at an affordable cost.

Organizations have four main tools for managing supply chain cybersecurity risks:

- Vendor qualification (including initial and periodic audits)
- Contracts
- Access controls
- Insurance

Suppliers pose a cybersecurity risk if they create, modify, maintain, archive, retrieve or transmit an organization's data. They also pose a cybersecurity risk if they provide or have access to the information systems of an organization or its suppliers.

How far down the supply chain should an organization go in managing its cybersecurity risks? The most common answer to this question is to focus on the first level of suppliers and require them by contract to take responsibility for their own suppliers. Within the first level, some suppliers will pose greater risks than others. On the other hand, some second-level suppliers may pose enough of risk to justify audits.

Regulatory Compliance

Supply chain cybersecurity breaches can violate a patchwork of regulatory compliance laws, such as the following:

- The U.S. Health Insurance Portability and Accountability Act (HIPAA) requires covered entities to enter into business associate agreements with third parties that will receive or be provided access to protected health information.
- FDA's regulation, 21 CFR Part 11 Electronic Records and Signatures, requires computer systems used to collect and analyze data in research conducted under an approved IND or IDE to be validated to meet requirements for electronic records and signatures.
- The California Consumer Privacy Act of 2018 (CCPA) requires a written contract, such as a service agreement, between a covered business and its service provider (Cal. Civ. Code § 1798.140(v).
- The European Union's General Data Protection Regulation (GDPR) takes a strict and more direct approach to contracts. If the organization is subject to the GDPR, it must have a written data-processing agreement in place with all its data processors. An organization must therefore understand the type and nature of data it is collecting to accurately determine the type of contractual obligations it can require of others and, in some instances, which obligations it needs to assume.

Do not assume liability beyond what is required (e.g., by signing a business associate agreement when no personal health information is being exchanged or where HIPAA does not apply). Knowledgeable legal counsel that understands the nature of data and how that data impact legal obligations and the particulars of the organization is more important than ever.

Managing Supply Chain Cybersecurity Risks with Risk Assessments

A supply chain cybersecurity risk management program includes the following steps:

- Identify the information that must be protected;
- Estimate the value of the information;
- Estimate the damage that would be caused by the loss, disclosure or compromise of the information;
- Assess internal processes and systems that protect the information;
- Identify who is responsible for protecting the information;
- Establish a program of internal security audits;
- Determine how security incidents will be identified and what actions will be taken to minimize the damage;
- Identify information that suppliers must be able to access;

- Assess ways to give suppliers access to the information;
- Assess the costs and risks of giving suppliers access to the information;
- Identify ways to mitigate the risks; and
- Rank suppliers based on their level of risk, likelihood of a security incident and the damage that would ensue.

Managing Supply Chain Cybersecurity Risks with Contracts

First, some caveats: Cybersecurity liability is a rapidly evolving legal area, as are related areas, such as privacy; so a contract drafted this year may be obsolete by next year. In the case of a security breach, establishing actual damages and allocating responsibility may not be straightforward, especially if the breach occurred at a lower level of the supply chain. Legal fees could be onerous, and a responsible party may not be able to pay.

Supplier contracts should include the following elements related to cybersecurity:

- Definitions of "data," "personal data," "data law," "data subject," "security incident," "security technical controls" and related terms
- A confidentiality clause that specifies the nature and type of data that are implicated by data privacy and cybersecurity provisions and types of confidential documents, information and intellectual property; how confidential items should be handled by both parties; and the consequences of a mishandling a confidential item
- A clause that covers data misuse by the supplier itself (including its personnel)
- A clause triggered by misuse or a security-breach incident, including requirements and notice obligations; the amount of assistance required of the supplier; and the liability associated therewith
- A clause that addresses the issue of the supplier's suppliers, including their access rights, chain of custody, and the supplier's obligations to protect the customer's data with its suppliers
- A clause that covers regulatory obligations
- A clause that covers both parties' rights and obligations related to supplier audit
- A "reasonable person" clause that, for example, states that a document that a reasonable person would assume is confidential does not have to be marked confidential to be treated as confidential

Managing Supply Chain Cybersecurity Risks with Supplier Assessments and Audits

A cybersecurity risk assessment involves asking a supplier questions about its cybersecurity processes, systems, and so forth; forming a judgment as to their adequacy; identifying ways to address any shortcomings; and determining whether the cybersecurity risk is acceptable.

A cybersecurity audit involves probing deeply into a supplier's processes, systems, and so forth by visiting facilities, examining documents, and interviewing responsible personnel.

A supplier assessment and audit program should include the following actions:

- Define the program's objectives, priorities, guidelines, criteria, processes, systems, timelines, measures of effectiveness, budgets, responsibilities and consequences.
- Perform assessments.
- Perform audits.

- Assess the effectiveness of the assessment and auditing program.

Internal personnel may conduct supplier assessments and audits, provided they have the cybersecurity expertise demanded by the risks. However, cybersecurity consultants can offer the following advantages:

- Experience and specialized knowledge
- Timeliness when internal personnel have conflicting priorities
- Objectivity under management pressure and questions about accountability

However, cybersecurity consultants bring with them their own cybersecurity risks. They should, therefore, be reputable, bonded and insured, and should minimize risks associated with their own repository of confidential documents.

Conclusion

Supply chain cybersecurity risks in clinical research can only grow as electronic systems replace paper and hackers become more sophisticated. Any weak link in the chain can create a widespread security breach with severe consequences. The only defense is a comprehensive and diligent program of risk management, a significant challenge given the growing cost and complexity of clinical research. When selecting suppliers, cybersecurity is a more important criterion than ever to consider.

References

1. Oladimeji, Saheed; Kerner, Sean Michael, "SolarWinds Hack Explained: Everything You Need to Know," (*WhatIs.com*, June 16, 2021), https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know.
2. Mitchell, Hannah, "California Hospital Patients' PHI Accidentally Posted Online for More Than 1 Year," (*Becker's Health IT*, April 26th, 2021), https://www.beckershospitalreview.com/cybersecurity/california-hospital-patients-phi-accidentally-posted-online-for-more-than-1-year.html.
3. Mitchell, Hannah, "4 Hospitals Added to CaptureRx Victim Tally: 21 Hospitals, Healthcare Organizations Affected," (*Becker's Health IT*, June 22, 2021), https://www.beckershospitalreview.com/cybersecurity/4-hospitals-added-to-capturerx-victim-tally-21-hospitals-healthcare-organizations-affected.html.
4. Terry, Mark, "Clinical Trial Software Company Hit by Massive Ransomware Attack," *(BioSpace*, Oct. 5, 2020), https://www.biospace.com/article/clinical-trial-software-company-eresearchtechnology-hit-by-ransomware-attack.
5. "SecureLink and Ponemon Institute Research Finds Remote Access is Becoming an Organization's Weakest Attack Surface," Ponemon Institute, May 4, 2021, https://www.securelink.com/news/51-of-organizations-have-experienced-a-data-breach-caused-by-a-third-party-new-report-finds.

Author

Rebecca Rakoski, JD, is co-founder and managing partner of XPAN Law Partners. Contact her at rrakoski@xpanlawpartners.com.