Berkleylifesciences
a W. R. Berkley Company

Outsourcing of Digital Information: What's the Problem?

Every day, there seems to be another headline of an information security breach at an organization. The latest big breach was when the government's personnel records of more than 14 million federal employees were taken from the Office of Personnel management by the government's outsourced contractors.[1] The government is not the only organization that has outsourced various internal functions, such as information technology (IT) and data management, to third party contractors. There are many reasons that companies outsource services including cost savings, inadequate staff resources, and volumes of information too large to effectively manage. Third party contractors help companies efficiently manage these services.

However, for life sciences companies, outsourcing can become a big liability because much of the digital information that these companies store, whether private patient health information or intellectual property, is sensitive in nature.[2] Therefore, it is crucial to understand the exposures around information security when outsourcing services and how to mitigate these exposures in your information security policies for third party contractors. This paper provides a review of what makes outsourcing digital information vulnerable for a life sciences company and how to choose third party contractors that will work with your policies and procedures. This is the second in a series of papers on cyber security in the life sciences space.

Understanding the vulnerabilities

The exposures that surround information security when services are outsourced are not straightforward and will need to be reviewed carefully to be identified. There are many ways that digital information can be compromised when services are outsourced. The following are some examples:

1. Cloud computing: "Software as a service" or subscription software where a vendor hosts its own solution and its customers access their separate accounts.
2. Managed services: When a customer relies upon its managed service vendor to provide not only the IT service but often the hardware as well.
3. IT contractors: Provides IT related work, such as data programming, data storage, web hosting, security, and helpdesk functions.
4. Contract research organizations: Conducts research work for the company using the company's intellectual property and manages the company's digital information associated with that research.
5. Outsourced contractors: An electrical contractor works on the hospital's digital network that then gains access to the digital network. These could be either direct contractors for the hospital itself or contractors for one of its vendors, like an outsourced lab.

With digital information outsourcing, there are more touch points with the data, so that the information is more susceptible to being breached. These extended relationships make it that much more challenging to control how the company's digital information is managed. Each outsourcing relationship should be analyzed and the contracts written in a way that spells out how the life science company's digital world is protected and clearly identifies the roles and responsibilities for data integrity.

Below are a series of questions about a digital information network that a company can consider using to understand where they might be vulnerable:

1. Do you know which data is sensitive or confidential? Is it isolated to ensure that access is not inadvertently granted? Is the data encrypted in any way?
2. Does the contract with your third party vendors include indemnity provisions that protect you from liability arising out of their loss of your sensitive information?
3. What types of controls has the vendor implemented to protect digital information?

4. How transparent will your vendor be about their processes so that you understand what happens to your digital information?
5. Does the vendor have a robust response plan in place in the event of a breach?

Risk Management Resources to Mitigate This Exposure to Cyber Security

To understand where to start in mitigating this exposure, a life sciences company should conduct a risk assessment of its information security policies and procedures around outsourcing to better understand its exposure and where to focus their mitigation efforts. The following practices can help a company reduce these exposures to cyber security:

1. Data mapping: Understanding what data is being outsourced and how it moves through the digital network will help you locate vulnerabilities. The path that data takes should be as controlled as possible whether by access control, encryption, or obfuscation (sanitizing or de-identifying the data). To do this, prioritize the steps that are taken and put in the controls starting with the highest priority. One example of technology that can assist with this process is data loss prevention (DLP), which helps to track data through this network and to control how the data is classified, protected, and where it cannot go.[3]

2. Service Providers: There needs to be transparency between the life sciences company and all of the service providers that it uses, including any sub-contractors used by the primary service provider. You need to know everyone who touches the data (or who can touch the data) and needs to ensure that all providers understand the protocols and procedures that have been put in place with the primary service provider.
    a. Provider selection process: When selecting outsourced service providers, develop a list of qualifications that your company requires for this provider based on your needs and vulnerabilities. Also, provide a questionnaire to the service provider to see how they ensure data privacy and security to see that it meets your company's needs. Some sample questions to ask are:
        i. Does your company have a corporate data security policy? If so, can you provide us a copy?
        ii. Are your systems subjected to penetration testing? Is this testing performed by internal personnel or outsourced? When was the last test? What were the results?
        iii. Other than penetration testing, have additional security assessments been performed on your systems? If so, when? What were the results?
        iv. Does your organization scan and/or test for vulnerabilities in your service/application, and if so, how quickly are any identified vulnerabilities remediated? Please provide as much detail in your answer as possible.
        v. How is physical access to your data center or any location where our data is stored secured?
    b. Contract Management: To further ensure that the service providers are following the data management procedures and controls, having solid contract language that outlines the responsibilities and the liability of the parties is necessary to ensure that the life sciences company is protected. The scope of the contract should also include what type of data is being passed through a given provider.
    c. Security audits: Each provider (primary and subs) will be audited on a regular basis to ensure that the security protocols are being followed. In addition, the data protection control methods that are being utilized will be checked to ensure that the company's data is protected in the manner in which it was outlined in the contract. Based on the type of data that the service provider or sub-contractor is processing, the frequency and depth of audits could change. Therefore, if the data is more sensitive, then the reviews should be more frequent.
    d. Breach response plan: The service provider should have in place a plan to be implemented if a breach happens at a customer's site. This is separate from a life sciences company's business continuity plan.

3. Business Continuity Plan: It is important that once your digital network has been identified and managed, a contingency plan be created, in case something does happen to either your network or that of your providers. The best way to do this is to think of what types of crisis could happen and how the company can respond to these situations. Once these have been determined, the company needs to find the gaps and detail an appropriate response. Some examples may be that the company does not over depend on one service provider and to protect the data servers with back up options.

Sonia Weiss, ARM, CIH, MBA, MPH, Senior Life Science Risk Management Specialist

Sonia Weiss has over 10 years of experience working in the environmental, health and safety ("EHS") professions, specializing in providing EHS services and advice to the academia, manufacturing, and biotechnology sectors. At Berkley Life Sciences, her focus is on helping her life science clients understand and manage their overall risk, with a particular focus on cyber security risk. Prior to joining Berkley Life Sciences in 2013, Ms. Weiss was the Safety Health and Environmental (SHE) Manager for Genencor, where she was responsible for workplace safety, regulatory compliance, risk assessments, and industrial hygiene. Ms. Weiss has a Bachelor of Arts degree in Biochemistry and Environmental Sciences from Northwestern University, a Master in Public Health in Environmental Health Sciences from the University of California, Berkeley and a Master in Business Administration from Presidio Graduate School.

[1] http://www.businessinsider.com/the-us-agency-plundered-by-chinese-hackers-made-one-of-the-dumbest-security-moves-possible-2015-6

[2] "4 IT Outsourcing Risks and How to Mitigate Them", available at http://deloitte.wsj.com/cio/2012/07/10/it-outsourcing-4-serious-risks-and-ways-to-mitigate-them/

[3] "Managing IT Risks in Life Sciences", available at http://deloitte.wsj.com/cio/2013/03/22/managing-it-risks-in-life-sciences/