Why Include Cybersecurity as part of GXP Vendor Qualification.

Third Party Risk Management, Part I

Paul Steiner, Ph.D., CQA
Steiner Consulting
pasteiner11411@gmail.com

Thomas Lee, Ph.D.
VivoSecurity
ThomasL@VivoSecurity.com

Abstract

QA (Quality Assurance) is often tasked with assessing GXP (Good *Manufacturing* Practices, Good *Laboratory* Practices etc.) compliance as part of vendor qualification. This qualification must include the vendor's ability to ensure data integrity as described by 21 CFR Part 11. Data integrity is an important component of cybersecurity, but QA teams in a pharmaceutical or biotech company are not comfortable assessing cybersecurity *per se* due to a lack of expertise.

Recently empirical regression models have become available which can objectively and accurately assess a company's probability for having a data breach. Although data breach is another aspect of cybersecurity, these models are simple to apply and provide an objective view of whether the cybersecurity team is adequately resourced and trained to carry out all aspects of cybersecurity including mitigating the risk to data integrity, and whether management culture supports compliance with policies and procedures.

These models can support a compelling argument for qualifying or disqualifying a vendor that must be able to carry out GXP functions, by objectively assessing a vendor's ability to maintain the integrity of electronic signatures and GXP records.

These models also accurately quantify the risk for a data breach and allow disqualification based upon a vendor's inability to ensure the integrity and privacy of protected data and your corporate secrets.

Article

Third party services (or vendors) have brought new efficiencies to companies. These services include outsourced manufacturing, many different kinds of consulting services, and cloud-based services such as Infrastructure as a Services (IaaS) such as AWS; Platform as a Services (PaaS) such as Heroku, Microsoft, Google, IBM; and Software as a Services (SaaS) such as HR systems, Electronic Medical Records, Document Control Systems, CAPA systems, and LIMS. But these services have also brought new risks, and now perhaps half of a company's risk is from

3rd parties. The FDA has recognized this and recently increased compliance requirements with a focus towards the challenges particular to 3rd parties.

In a pharmaceutical or biotech company, a serious risk is noncompliance with GXP as described by 21 CFR 820. The QA group performs pre-contract qualification activity for any 3rd party that will be part of GXP activities. Third parties might include laboratories, drug manufacturing facilities and cloud services that might maintain or manage electronic records involved with GXP activities.

Qualification includes data integrity per 21 CFR Part 11 (Part 11), which is also an important component of cybersecurity. Cybersecurity includes much more than simply data integrity, for example, data breach is a major concern of cybersecurity.

Recently new tools have become available that objectively and accurately forecast probability for data breach, bring new insights into the problem and make it easy for the non-expert to assess the cybersecurity of 3rd parties. We argue for including these tools as part of vendor qualification. We see three main values:

- Including cybersecurity using the new tools will give QA additional objective leverage to qualify or disqualify a vendor and to pressure a vendor to make needed changes.
- Including cybersecurity using the new tools will give QA a more comprehensive and objective view of the vendor's interest in good policies and procedures in general, and in supporting Part 11 in particular.
- Including cybersecurity will show regulators that your company has a mature and comprehensive TPRM (Third Party Risk Management) program. It will also protect your company against data breach risks, including loss of intellectual property and risk from exposing patient or clinical trial data.

We will expand upon these arguments in reverse order below.

Comprehensive and Mature TPRM program

The current method for assessing the security posture of 3rd parties is to use questionnaires and maturity scores or through limited physical inspection during routine or “for cause” quality audits. However, these methods are largely subjective and don’t directly answer the business question: can this 3rd party partner cause a data breach of our data? It is also hard to understand the technical questions, the answers to questions or even the importance of the questions.

Recently, empirical regression models have become available that accurately forecast the probability for data breach based upon—not security controls, but upon the number of trained cybersecurity employees and the number of audit and compliance employees. “Empirical” means that these models are not based upon opinion like the current questionnaires, but upon predictive factors that were discovered. These models also meet The Federal Reserve and

Office of the Comptroller of the Currency supervisory guidance, SR 11-7, used in the financial industry for assessing, for example, credit risk.

It should be as no surprise that headcounts of trained employees normalized by company size or IT size can be used to forecast data breaches. Companies use standard technologies and applications, and the practice of securing these technologies and applications is standard. Indeed, counting the number of employees trained in these standard controls that are involved with discovering risk, deploying, configuring and monitoring standard controls, writing policies and procedures is very accurate at predicting data breach.

Using headcounts is not that different from the method that some QA people use for an initial assessment during a Quality System audit of, for example, a manufacturing facility: count the number of QA people and normalize by the number of technical people at the facility. The result of this exercise would then guide the QA audit team in what areas to focus during the audit.

The most important reason for using these new tools is because the probability for a 3rd party data breach is a function of the number of 3rd parties and maturity scores or a review of security controls through questionnaires does not measure this aggregate risk. Aggregate risk is always much greater than the risk from any single 3rd party partner. As an example, if the likelihood of a data breach for a 3rd party is once in 100-years, then the aggregate risk among ten similar 3rd parties is once in 10-years.

Aggregate 3rd party probability for a data breach may be calculated by simply summing probabilities for the individual 3rd parties. The new empirical regression models calculate probabilities as a function of data breach size, thus allowing forecasting aggregate probability for data breach based upon data breach size.

Although QA faces FDA regulators, their company is also obligated to secure PHI (Protected Health Information), regulated by another branch of the federal government: Health and Human Services (HHS) and the Office of Civil rights (OCR). The ability of the vendor to secure and maintain PHI records should be part of the consideration in qualifying the vendor. Specifically, the Health and Human Services regulation 45 CFR 164.308 (see also) states “Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate”. Failing to accurately assess a new vendor as part of an aggregate risk assessment is a compliance failure. The new models simplify this process, while also quantifying the aggregate probability for data breach and bringing new insights into a company's ability to be Part 11 compliant.

Mature *Third Party Risk Management (*TPRM) programs consider all major risks to a company. We recommend that QA include the risk of data breach when they qualify a GXP vendor. Identifying and mitigating deficiencies for all significant risks before signing a contract is best practice TPRM across all industries.

Good Compliance Culture

Compliance with good policies and procedures is a foundation of GXP and fundamental to electronic signatures (Part 11). Electronic signatures are often implemented with *Microsoft Active Directory* and depend on the IT and HR departments following their *Standard Operating Procedures*, and employees following their training.

Audit and compliance were also found to be very important at reducing probability for data breach. Empirical regression modeling found that the number of trained and certified audit and compliance employees was just as effective at reducing probability of data breach as the number of trained and certified cybersecurity employees. This is a big surprise to the cybersecurity industry which has overfocused on measuring the presence of cybersecurity controls to assess 3rd parties.

Perhaps the importance of compliance should not be a surprise, since data breach can happen in many different ways: accidents, lost/stolen devices, malicious insiders, and malicious outsiders, and it is prevented by IT and cybersecurity departments following their *Standard Operating Procedures* and by employees following their training.

Empirical regression models would seem to be teaching us that this compliance, needed for both Part 11 and for preventing data breach, can be objectively measured simply by counting the number of auditors within a company.

Therefore, an important reason for QA to include cybersecurity as part of their qualification is that it provides an objective measure of both a company's audit and compliance culture and cybersecurity strength. Data integrity is an important part of cybersecurity. Data integrity and compliance are both important for Part 11 and electronic signatures. Modeling results from cybersecurity might therefore be used to inform how qualification audits are performed and underscore GXP related deficiencies found.

Argument for Disqualification, leverage for addressing deficiencies

Finally, including cybersecurity and probability for data breach as part of 3rd party GXP qualification gives additional leverage within your company for qualification or disqualification. It can also provide compelling information to convince a 3rd party to address deficiencies.

Again, including cybersecurity as part of qualification is justified since data integrity is an important part of cybersecurity and essential for meeting Part 11.

Following are the underlying reasons that collectively form the basis for disqualification:

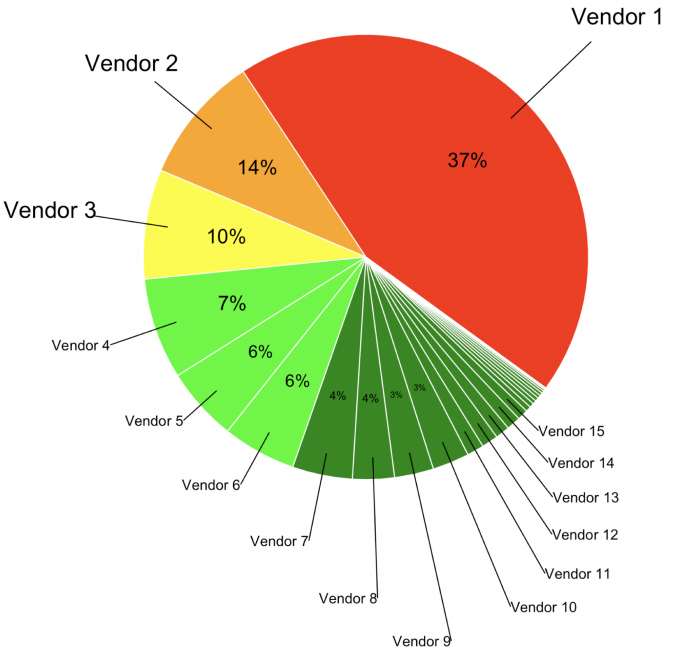
1. 45 CFR 164.30 requires an ***accurate and thorough*** cybersecurity assessment which must therefore include aggregate risk in order to be valid,
2. Senior management and the board of directors has a **fiduciary duty** to decide an acceptable aggregate risk appetite,
3. Generally, just **one or two 3rd parties** can cause this aggregate risk appetite goal to be missed.

The table and pie chart below help to illustrate this strategy. The table below shows aggregate probabilities for a biotech company with thirty-two 3rd party partners that could expose data. The table shows, for example, that there is a once in 4-year likelihood of one of the 3rd parties having a data breach affecting 100,000 people. The table also shows that this is significantly higher than a cross industry median, which is once in 13 years.

Breach Size (People Affected)	Aggregate Breach Frequency (annual probability)	
	Company	Industry Median (σ)
100,000	4-years (25%)	13-years (10) (8%)
1,000,000	11-years (9%)	43-years (42) (2%)
10,000,000	89-years (1.1%)	374-years (324) (0.3%)
100,000,000	474-years (0.2%)	2356-years (2273) (0.04%)

Senior management and the board of directors should decide if these data breach frequencies are acceptable or if different goals should be set.

The pie chart shows a breakdown of each vendor's contribution to this aggregate risk, for a data breach affecting 100,000 people. Each slice is a different vendor, but vendors have not been identified because this is a snapshot in time and some vendors have reduced their cybersecurity risk. The pie chart shows that just two vendors: Vendor-1 and Vendor-2, represent half of the risk (37% + 14% = 51%). Giving these two vendors access to PHI data has therefore doubled the aggregate risk from a once in 8-year frequency to the current once in 4-year frequency. If management had set a risk appetite goal of once in 8-years, it would be hard to justify accepting these two vendors without a significant change in their security posture. It would be difficult to challenge the aggregate data breach forecast since the models are accurate, make a testable forecast and are based upon headcounts which would show obvious deficiencies.



Companies that make a large contribution to aggregate risk also tend to be companies with weak audit and compliance cultures which is a clear GXP risk. The combination of GXP risk and the increase in likelihood for a 3rd party data breach, perhaps at a level already deemed unacceptable by corporate leadership or the board of directors would justify disqualification.

Comprehensive Series of White Papers

This is the first in a series of white papers that discuss how these new models help the QA teams in biotech and pharmaceutical companies tackle major risks from 3rd parties. Future papers will cover how these models can be leveraged in CAPA response to a 3rd party data breach and how these models can be used to compare 3rd party partners.

About the Authors

Paul A. Steiner Ph.D, CQA has a consulting business providing services in the areas of pharmaceuticals (GMP, GCP, GLP, GPVP) and medical devices with emphasis on quality systems, regulatory compliance, supplier qualification audits, chemical, manufacturing and control (CMC) and materials and process science (Advanced fiber composites and adhesives). Often serving as an expert witness in his consulting roles, he is also an ASQ CQA (certified quality auditor). He has performed over 200-300 audits spread over four continents in his career to date, primarily as lead auditor.

Before going into business for himself, Paul A. Steiner was the Head of Quality at the last few pharmaceutical companies for which he worked. He has worked in quality assurance (QA) in pharmaceutical / biopharmaceutical and medical device companies some of which included, Gilead, FibroGen, NGM Biopharmaceuticals, Vivus, and Affymetrix (recently acquired by Thermo Fisher) to name a few. With a Ph.D. in organic chemistry from the University of Washington and an undergraduate degree in chemistry and chemical engineering from Cornell University, he started his career at Bio-Rad Laboratories as a scientist working in R&D and process development/engineering. With roles of increasing responsibility in technical management, he spent most of his career working for companies which were to some degree “virtual” managing third-party contractors. Dr. Steiner has technical and management experience spanning all phases of the product lifecycle from early research and development through cGMP quality operations.

Thomas Lee Ph.D is the CEO of the Silicon Valley based **VivoSecurity**, a company focused on data collection, regression modeling and AI to quantify cyber security risk. Thomas has spoken at the Richmond Fed research conference 2018, invited participant at Richmond Fed cyber security workshop 2019, invited speaker at O.R.X Toronto & Milan 2018, speaker at OpRisk North America 2018, ACAMS panelist 2019, PRMIA NYC & BCG 2018, multiple patents for quantifying cyber security risk. Thomas holds degrees in Physics and Electrical Engineering from the University of Washington in Seattle, and an MS and PhD in Biophysics from the University of Chicago.

If you are interested in obtaining an electronic version of this white paper, please scan the code to the right.