Risk Bulletin

Key insights to help your organization manage risk and make timely decisions

Fall 2014

Size doesn't matter: The anatomy of a data breach

You may think you are too small to suffer a data breach. Think again.

The threat of a data breach is rising as all information has value to hackers. Incidents occur regardless of an organization's industry or size, and small and midsize businesses are particularly at risk due to generally weaker security and controls. This infographic illustrates how hackers exploit vulnerabilities, the damage a data breach can do to your business and how you can protect yourself.

Are you concerned about your data security and vulnerability to a data breach? Learn more about how McGladrey's security and privacy *Rapid Assessment*® can identify your control gaps and help protect your organization.

Download the infographic.

Simplify the complexity of third-party management

Corporations continue to increase their use of third parties, depending on countless vendors, suppliers, distributors and contractors throughout their value chain. While the use of these organizations is increasingly critical for success, third parties can leave you vulnerable to greater financial, regulatory and reputational risks unless you have the right attention and processes. As these relationships become more commonplace and more strategic, regulatory bodies are paying closer attention, with increased pressure and penalties.

The use of third parties has increased for several reasons, including the ability to scale rapidly, raising capacity to meet demand. Third parties can also provide increased access for organizations seeking an international presence. The right strategy can bring products to market more efficiently; instead of building costly infrastructure, organizations can partner with data centers and application providers to enhance technology resources.

Third-party risk management has been addressed in a siloed and limited fashion for most organizations. However, increased reliance on third parties is causing companies to review their policies and strive for a more holistic approach. For example, data privacy is a key concern amid breaches and increased hacker activity; comprehensive processes that identify and actively manage all vendors that have access to sensitive information are therefore required. If an incident occurs, it does not matter if your third-party is the cause; you retain ultimate responsibility and your company's brand is the one that is tarnished.

The elements of an effective third-party management program

Developing a strong third-party management process can be a complex endeavor. Each pillar is dependent on sufficient resources to support the infrastructure, consisting of the right people, processes and technology. Contrary to popular belief, a significant expense is not always necessary, but you need to think through the skill sets of the people that you need and ensure that processes flow appropriately to accomplish their desired goals. Technology allows you to leverage the program across your organization.

Planning

Before you select a third-party, you should complete a thorough planning phase. Planning assumes that you understand the inherent risks that your organization faces when utilizing a third-party. Begin with a high-level business case, assessing alignment with strategy and other priorities, such as information technology development or mergers and acquisitions. Evaluate what functions you need to outsource, the customer and employee impact if you do so and plan for managing related risks. Only after those steps have taken place should you review the marketplace for qualified third parties.

Due diligence

Performing third-party due diligence involves several steps common to the typical procurement process, including issuing a request for proposal (RFP), ensuring the third-party is qualified and that service-level agreements are in place. However, you must also link your inherent risks (identified in the planning stage) back to the due diligence process to ensure that a potential third-party has appropriate controls in place to mitigate the relevant risks. In addition, due diligence should include reviewing system architecture, establishing and visiting service locations and assessing reliance on subcontractors.

Risk assessment

To effectively assess risk, you should conduct detailed controls assessments of RFP finalists, perform reference calls and background checks. Assess a third-party's control effectiveness based on provided responses, documentation and site visits, as applicable.

Contract negotiation

After analyzing inherent risks and determining potential vendors' controls and comparing them to your needs, link this information to contract negotiations to ensure your gaps (in terms of identified risks) are covered. Contract clauses should directly reflect identified and understood risks. Retain a short list of third parties to maximize leverage on terms and incorporate RFP responses regarding standard terms into the negotiation. Make a final selection based on your total cost of ownership (including risk management) and contractual terms and obtain any required approvals.

Establish a vendor management program

Formulate a plan for each particular third-party with whom you do business. The level of required oversight for performance and financial reviews will differ between third parties; some require more significant attention, while others need lighter oversight. Map contractual commitments and residual risk mitigation strategies to third-party management plan activities. Remember that the risks you are assessing, the controls in place and the action plans you establish must be relevant to each particular third-party.

Ongoing monitoring and assessment

On an ongoing basis, execute on your third-party management plan activities and periodically reassess risk. Consistently execute your decisions, to demonstrate the plan for auditors or regulators. Escalate any increased risk or deterioration of performance and execute on governance and reporting.

Contract termination

When planning, you must identify issues and strategies for contract termination. Nobody wants to think about it, but it does happen, and both parties must be protected. Detail an orderly transition in-house or to an alternate third-party, based on contractual commitments. Assess risk and ensure return or confirmation of destruction of confidential information. Also address ownership of joint intellectual property.

Additional considerations

Any program must have oversight and accountability from executives and the board, not just internal audit and risk management. In addition, you must have sufficient documentation and reporting to store information and organize it to be accessed and reported on quickly. Lastly, independent reviews are necessary to analyze your program and address evolving regulations, laws and risks and to enhance processes.

Tools to enable your program

Your program must be flexible enough to be commensurate with the inherent risks in each engagement. You cannot manage every risk with every third-party in the same manner. As you think about developing your process, focus on consistent methodology, a contract repository, appropriate workflows and a platform that enables you to track and report on all activities for regulators and the board.

Retain electronic images of contracts, as well as a repository for responses. Maintain a consistent, documented algorithm for calculation of aggregate inherent and residual risk and a tracking mechanism of those calculate risk ratings, as well as action items by third-party, relationship and segment. Finally, implement a performance management system to enable program-level reporting of adherence to contractual service levels and highlight degradation of performance.

Critical success factors

You must establish who owns the process and obtain buy-in from leadership to gain support for decisions and to establish goals. A centralized process typically works best, but no one size fits all. Develop a risk assessment that matches your overall risk profile and includes a complete list of third-party relationships. Implement an ongoing monitoring and review program to review documentation that is obtained and ensure it is appropriate and current.

Simplify the complexity of third-party management, continued on page 3

Simplify the complexity of third-party management, continued from page 2

To get started, review your current program to identify gaps and apprise the board and senior management of the need for increased involvement. Develop a detailed plan, schedule and budget to address these gaps and policy, process and technology requirements. Coordinate independent review needs with audit and broaden your view to incorporate strategic, regulatory and other third-party risk expectations that could be addressed simultaneously.

Regulatory changes are inevitable, and your ability to adapt is critical. Your third-party management policies and processes are only half of the battle; consistent execution and evidence are also key. Your third-party management solution must be scalable to accommodate increasing depth and breadth of review, usable by a distributed network of stakeholders, easily configurable by business users and IT programmers and fully adaptable, transparent and comprehensive.

View the recorded webcast:
Simplify the complexity of third-party management

Information security due diligence – Did you buy an asset or a headache?

According to Bloomberg's Global Financial Advisory Mergers and Acquisitions Rankings Q3 2013, mergers and acquisitions increased 33 percent in 2013. Of particular interest is technology sector activity, which was at a five-year high during the third quarter of 2013, leading to buyers paying the highest premium on technology companies. Purchasing high-premium companies typically includes intellectual property, private information databases (big data), source code, critical systems and trade secrets, among other items. However, there is a unique threat to these types of assets in that they can be stolen or subverted without the data owner's knowledge and often leave little evidence that the asset has been compromised.

While high profile news stories are published about data thefts from large organizations and retailers, many more data breaches occur that are not disclosed or aren't deemed appealing enough to get articles written about them. According to www.datalossdb.org, an open-source data breach tracking database, over 2,200 companies experienced data breaches of protected personally identifiable information (PII) during 2013. Most of the breaches occurred at midsize and smaller organizations. The 2013 Verizon data breach report (a study of trends in data breaches investigated by 19 different forensic investigation companies) indicated that over 65 percent of the data breaches investigated were at companies with less than 10,000 employees. Oftentimes, midsize to smaller organizations have weaker protections on their data and are easier targets. The report also documented that for 66 percent of the investigated breaches, compromised organizations did not discover the intrusion for a period of multiple months to years after the initial compromise. This lengthy timeline to discover a breach resulted from the fact that almost 70 percent of the breaches were discovered by third parties, rather than the organizations themselves.

In one example, Nortel was penetrated by hackers prior to declaring bankruptcy. By the time the hackers were discovered, it was determined that they'd had access to Nortel's data for almost 10 years and had stolen business plans, research and development papers, emails and technical papers. Once the breach was discovered, management cut off the attack, but reportedly chose not to follow up with an investigation – or disclose the breach to the companies buying its $4.5 billion worth of patents. As a result, the attackers will probably never be identified and the companies acquired compromised systems that could be used to expand the attack into their networks. The purchasing companies would more than likely not have paid nearly as much for the intellectual property had they known about the breach prior to the purchase.

Typical due diligence performed on a potential acquisition is designed to make sure the asset is properly valued. Large amounts of data must be examined and assessed during the due diligence process, which typically occurs at a rapid pace. Financial audits are performed and basic controls reviews are sometimes conducted to substantiate the value of the purchase and the maturity of the operation. However, one must consider that if a large percentage of breaches go undetected for months or years at a time, a review of the standard operating controls will not detect a breach either. If the potential acquisition does not have monitoring systems in place or, more commonly, if they are not effectively monitored by qualified individuals to detect unauthorized activity, the organization could have unknowingly lost critical data before the letter of intent was drafted.

If a potential acquisition includes significant electronic information assets, a review of its current information security maturity could have a large impact on the value of the assets. If data has truly been stolen, it is quite possible an empty asset would be acquired, or at least one

Information security due diligence, continued on page 4

Information security due diligence, continued from page 3

worth much less than initially believed. For instance, many social media companies' largest asset is their membership data. That data is proprietary and linked to creating customer profiles that business partners purchase. But, if that data has already been stolen, an attacker could sell the data at a fraction of the cost, dramatically affecting the potential earnings of the company. Other items, like intellectual property or custom source code, could create the same issue.

Even if an organization does not have secret data, most companies have some protected data, such as PII, ePHI, credit and debit card data or government data. The loss of this type of data would be embarrassing to the company and potentially create an immediate burden on its new owners or worst case, could force them to assume the liabilities associated with data loss in any of the protected classes.

So what can be done? Standard due diligence is unlikely to detect a data breach if the company has not detected the breach already. Companies can protect themselves by making sure that due diligence procedures include information security objectives, internal and external penetration tests and data identification procedures. If time permits, one of the most effective methods of detecting an attack is to monitor attempts by attackers to extract data from the environment. Proper monitoring of Internet connections can reveal whether data has been stolen or is in the process of being stolen, and depending on the logging available, could reveal how much data, if any, has been stolen so far. However, a detailed log review can take quite a while to complete and may take longer than desired for the purchase cycle. Thus, log reviews would only pertain to organizations where data compromise is already suspected.

While no due diligence is 100 percent effective in preventing the unforeseen, performing information security due diligence on potential acquisitions that have significant intellectual property, digital information assets or obviously lax information technology controls, can make the difference between a profitable transaction, a loss or a significant liability.

COSO Resource and Information Center

In 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published Internal Control-Integrated Framework, which has become commonly known as the COSO Framework. An updated Framework was issued in May 2013. It retains the original five components of internal control – control environment, risk assessment, information and communication, control activities and monitoring activities; however, it adds 17 principles and 81 points of focus that are necessary for an effective internal control environment. While the Framework provides guidelines, questions may still remain regarding the implementation of the new guidance.

How our COSO and internal control specialists can help

Our multidisciplinary team of specialists can assess your current internal controls landscape and collaborate with you to develop and execute a work plan unique to your situation, and help you optimally comply with the 2013 COSO Framework.

Visit our COSO Resource and Information Center for valuable information.

Overcoming hidden risks within construction contracts

While the funds for construction activity and capital projects are down in recent years, fraud has gradually increased in the construction industry. State and local government entities must implement measures to protect projects against fraudulent activity, ensuring they stay on time, on budget and deliver the expected quality. With more bids for fewer projects and large contracts at stake, you must be aware of warning signs to ensure contractors remain in compliance.

Common risk areas

A recent Association of Certified Fraud Examiners (AFCE) report found a median construction fraud loss of $300,000, the third highest amount of any industry. The most common fraudulent areas were billings (36 percent) and corruption (34 percent). In the case of billings, there is no penalty for overcharging a customer, and often, a contractor is only caught if an audit takes place.

Overcoming hidden risks within construction contracts, continued on page 5

Overcoming hidden risks within construction contracts, continued from page 4

The AFCE also pointed out several behavioral red flags to be cognizant of, including a close association with vendors, a "wheeler-dealer" attitude, excessive pressure and control issues. Each of these characteristics can be associated with construction companies, from both contractor and owner perspectives.

Typical contract structures

State and local government entities typically engage in two types of contracts, lump-sum (fixed-price) or cost-reimbursable projects. Your type of contract may be dictated by state or local regulations, but both carry various levels and areas of risk.

In a lump-sum contract, the project is competitively bid, as multiple offers are collected and the most competitive and responsive bid performs the project. This contract can also be negotiated, but is viewed as high risk for many reasons.

In a federal government environment, the Truth in Negotiation Act dictates that a contractor must provide documentation and information that is current, accurate and complete. Unfortunately, similar regulations do not exist in a state and local government setting. When negotiating, risks arise when the contractor may not provide all of the information and data that they are aware of and does not negotiate in good faith.

The next type of contract is cost-reimbursable, also known as cost-plus. These agreements exist in many different forms, including those paid with a fixed or a percentage fee. In the federal government, it must be a fixed fee, but most state and local entities enter into percentage fee agreements. Other forms of this contract are guaranteed maximum price agreements, as well as time and material contracts.

The type of contract you choose may be predicated on regulations you have to abide by, as well as by the type of project you require. In other words, if it is a simple design, you may want a lump-sum contract. However, if it is a more complex project, a cost-reimbursable contract may be more beneficial.

Knowing your risks

A construction project is a balancing act, with three primary areas to focus on: cost, schedule and quality. Each of these areas is interrelated and can directly influence each other; for example, some contracts may include incentives to complete a project early, impacting both schedule and cost. Unfortunately, the connected nature of projects leads to complex agreements and increases the potential for fraud.

Several unique risks are apparent within lump-sum contracts, such as:

- Procurement – Occasionally, the bid process is manipulated, or the lowest bid might not be the best bid.
- Specifications – Contractors may take shortcuts when they do the work.
- Change orders – Contractors make up for low bids by submitting change orders, and many have errors in their estimates or insufficient documentation.
- Front-end or top-loading – A contractor bills your organization in advance of performing the work.
- Allowances – Money is set aside for a specific task, but contractors use those funds for other tasks.
- Prevailing wage rates – In the public sector, contractors must meet wage requirements; however, many contractors do not adhere to guidelines.

Cost-reimbursable contracts also include several distinct risks that you must be aware of and manage, including:

- Labor – Many areas are prone to overbillings and risk, such as fringe benefits and worker's compensation.
- Cleanup – Subcontractors are normally responsible for cleanup, but contractors may submit excessive charges for providing services that are the responsibility of subcontractors.
- Negotiations – As mentioned earlier, some contractors fail to negotiate in good faith by not providing accurate and complete information.
- Subcontractor -- Contractors sometimes provide trade work, which is known as self-performed work. In these instances, the contractor manages their own work, potentially resulting in poor craftsmanship or excessive change orders.
- Insurance – Excessive costs and coverage charges are becoming more common due to recent changes in insurance coverage.

The majority of overbillings come from labor (51 percent), followed by insurance (21 percent), billings in excess (17 percent) and miscellaneous charges (10 percent). However, fraudulent charges related to insurance are rising and will become more prevalent in the coming years.

With tighter budgets and limited flexibility, state and local governments must perform due diligence to avoid overbillings and

Overcoming hidden risks within construction contracts, continued on page 6

Overcoming hidden risks within construction contracts, continued from page 5

fraud in construction projects. In many cases, internal controls must be implemented or adjusted to account for evolving risks. However, a construction audit is also a valuable tool to ensure costs are allowable and in accordance with the contract and to recover any potential overbillings.

800.274.3978
www.mcgladrey.com

Risk Bulletin
Fall 2014
Printed in U.S.A.