GoldSky Cyber Security | White Paper

3rd Party Vendor Risk Management

SERIES ONE

Rudy Silva, CISSP
SE Cybersecurity Practice Director

TABLE OF CONTENTS

01 INTRODUCTION

Businesses increasingly work with third parties in ways that can render otherwise well-protected data vulnerable to cyberattacks or accidental disclosure. These third parties oftentimes include technology service providers and/or vendors providing business functions, such as payroll and accounting; corporate insurance and benefits; legal services, etc.

Many of these commercial relationships require an exchange of sensitive information - whether confidential information pertaining to corporate employees, customers, or computing infrastructure - to be shared with, or stored by, the third parties. Such relationships also may entail third party's access to an organization's networks. There is, in turn, an inherent risk in the third-party services: new attack surfaces could compromise a company's data, its systems and networks - and those attack surfaces require appropriate mitigation.

In recent history, a major third party attack can be attributed to the events involving the U.S. retail company, Target. The Target security breach incident began not with a direct attack on the corporate network, but with a phishing attack against Target's third party HVAC contractor - this third party attack was leveraged against Target's external billing and project management portals.

The HVAC contractor depended on a free version of a consumer level anti-malware software, which allegedly failed to provide real-time protection. Once the phishing campaign succeeded in installing a key-logging malware, the malicious actors obtained the HVAC contractor's credentials to Target's external billing and project management systems. Then, the malicious actors infiltrated Target's internal network and by lateral movements, they were able to access Target's customer databases and point-of-sale systems.

Following the third party security breach that affected Target Corporation, the personal information of up to 70 million customers were compromised, and about 40 million customers had their payment card information stolen. By the end of 2014, the security incident recovery processes cost Target over $150 million. These costs included litigation and settlement expenses resulting from lawsuits lodged by consumers and credit card issuers. Furthermore, during the quarter when the data breach occurred, Target's year-over-year earnings plummeted by 46 percent. Ultimately, in the aftermath of the breach, Target's reputation was damaged and its CEO was forced to resign.

Unfortunately, the third party security incident which affected Target Corporation was not an isolated incident. In 2014, a Ponemon Institute survey found that in 20 percent of data breaches, a failure to properly vet a third-party, contributed to the breach. Even more troubling, 40 percent of the respondents to another Ponemon survey named third-party access to or management of sensitive data as one of the top two barriers to improving cybersecurity. Furthermore, the Ponemon Institute's 2015 U.S. Cost of Data Breach Study reports that third-party involvement in a data breach increased the per capita cost of data breaches more than any other factor. However, despite the cybersecurity risks posed by third-party service providers, many companies fail to systematically address such risks. Only 52 percent of companies surveyed in a 2014 Ponemon Institute report have a program in place to systematically manage third-party cybersecurity risk.

02 LEGAL RISKS

Although there are many commercial reasons to adopt strong third-party risk management processes, a variety of legal frameworks mandate the management of third party risks. Examples included below of such statutory or regulatory requirements.

INTERAGENCY GUIDELINES ESTABLISHING INFORMATION SECURITY STANDARDS

that implements Section 501 of the GrammLeach-Bliley Act (GLBA), which requires financial institutions to engage in due-diligence procedures when selecting third-party service providers. Some of these due-diligence procedures include the use of Service Level Agreements (SLAs) as a contractual provision to manage third party risks; monitoring and auditing of third-party service providers on an ongoing basis.

THE FEDERAL TRADE COMMISSION (FTC)

has exerted its authority under Section 5 of the FTC Act, 15 U.S.C. §45 (governing unfair acts and deceptive trade practices) to apply to data privacy and security. Thus, the FTC has taken action against companies that fail to take “reasonable steps to select and retain service providers capable of appropriately safeguarding personal information” as a de facto regulatory requirement.

STATE MANDATED DATA PRIVACY AND SECURITY REGULATIONS

such as the Massachusetts Standards for the Protection of Personal Information, which requires reasonable due-care during the selection of third-party partners. Additionally, this includes a requirement for the implementation of contractual provisions, which requires that third-party providers remain in compliance with the 201 Mass Code for the State of Massachusetts.

HIPAA PRIVACY RULE

which requires specific contractual provisions as well as data privacy and security best practices when handling protected health information.

The cybersecurity and privacy risks generated by third-party engagements include the following:

BREACH OF SENSITIVE DATA

This cybersecurity risk includes the potential theft, loss, and/or corruption of critical data pertaining to customers, employees, or competitive business intelligence. In several cases, this type of cybersecurity risk is categorized as ransomware attack.

Security incidents affecting business data are oftentimes handled with the utmost regulatory obligations, which includes the notification of affected individual parties - usually resulting in enormous ransom payments and legal liabilities.

MALWARE LATERAL MOVEMENT INTO CORPORATE NETWORKS

thus interfering with critical business operations. A recent example of this type of third-party cybersecurity risk was the Dairy Queen attack, in which a third-party service provider credentials were used to gain access to internal networks and eventually install malware targeting point-of-sale systems.

THE INTRODUCTION OF ZERO DAY VULNERABILITIES INTO IT SYSTEMS

For instance, if a third-party service provider is using unpatched application systems to access an organization's critical computing environment, then said vulnerable third-party applications system could create an attack surface that can be exploited by malicious actors - this third-party cybersecurity threat is oftentimes materialized in a Heartbleed OpenSSL exploit, where exposed data is transmitted between a secure web servers and a rogue command-and-control server.

THE MISUSE AND ABUSE OF SENSITIVE CORPORATE DATA

Suchgmai as for data mining, for the competitive benefit of a third-party service provider. This risk is a direct breach of fiduciary duty and disregard for the acceptable use policy of a third-party's clients. All in all, the misuse and abuse of sensitive corporate data creates a "fourth-party" risk, that is, the third party cybersecurity risks introduced by a vendor's relationships with its own third-party service providers and vendors.

To effectively manage this array of risks, organizations must assess the protective, defensive, and corrective controls within their organization. Secondly, the primary organization must ensure that there are appropriate procedures in-place to evaluate and monitor third-party service providers privileges, as well as a program to manage and monitor third-party relationships.

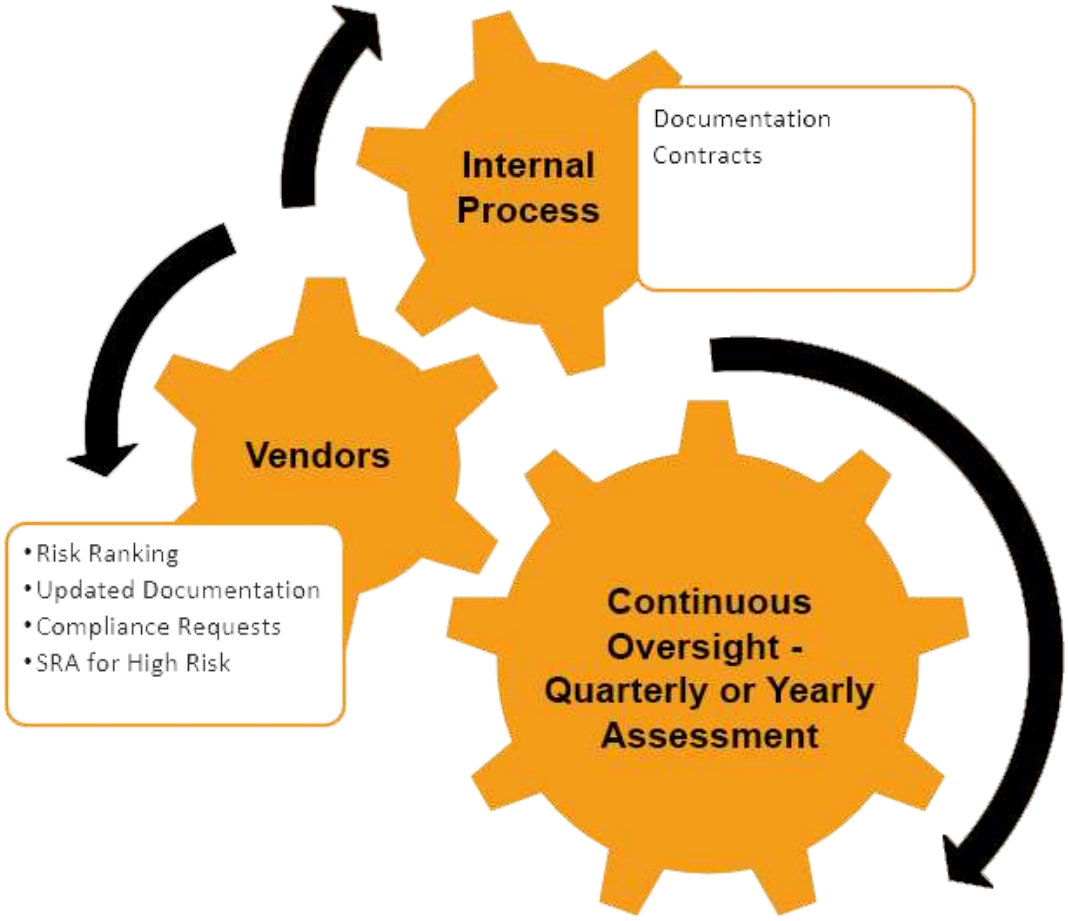
04 ENGAGEMENT-LEVEL MANAGEMENT OF THIRD-PARTY CYBERSECURITY RISK

The appropriate measures needed to scrutinize and monitor third-party service providers will depend, to a large extent, upon the sophistication of the third-party service provider and the nature of the IT systems and data in question.

Nonetheless, three elements are common to all third-party risk management:

A critical element of managing third-party risk is the assessment of the third party's own security practices and posture before any contract is signed. Such due-diligence is crucial for the identification and evaluation of risks, and, in turn, it ensures that such risks are mitigated before the business engagement. The actual evaluation may be more ad hoc (i.e., conversations with key business or technology stakeholders) or formal (i.e., through a questionnaire or even on-site assessments). The extent of a third-party evaluation may depend on various factors in the prospective relationship, including, for example, whether the service provider will have access to the company's IT systems, the nature of the information that it may access, and whether it will store such information.

04 ENGAGEMENT-LEVEL MANAGEMENT OF THIRD-PARTY CYBERSECURITY RISK



Third-Party Risk Management

Depending on the extent of the relationship and information that may be accessed by the third-party service provider, the following areas of inquiry may be necessary to inform a cybersecurity diligence assessment of third-party service providers:

04 ENGAGEMENT-LEVEL MANAGEMENT OF THIRD-PARTY CYBERSECURITY RISK

How often does the third-party service provider experience security incidents; severity of past security incidents; the quality of the incident response processes.

Determine whether the third-party service provider maintains written cybersecurity policies and action plans.

Organizational considerations, such as does the third-party service provider maintain sufficient and appropriately trained cybersecurity personnels to ensure the confidentiality, integrity, availability, and privacy of data and/or services.

Human resources practices, particularly background screening of employees, cybersecurity awareness training, and the handling of terminations.

Determine access control management procedures, particularly whether controls are in-place to restrict access to information and uniquely identify users - determine how often access control logs are monitored and reviewed.

Assess the encryption practices in-place, including the type of encryption protocols employed for data-at-rest and data-in-transit as well as the best practices for cryptographic key management.

Evaluate the data privacy and security laws of the country where data is being stored, and ensure that the third-party service provider addresses secondary usage of clients' data within their Cybersecurity policies. There must be limitations to secondary usage of data.

04 ENGAGEMENT-LEVEL MANAGEMENT OF THIRD-PARTY CYBERSECURITY RISK

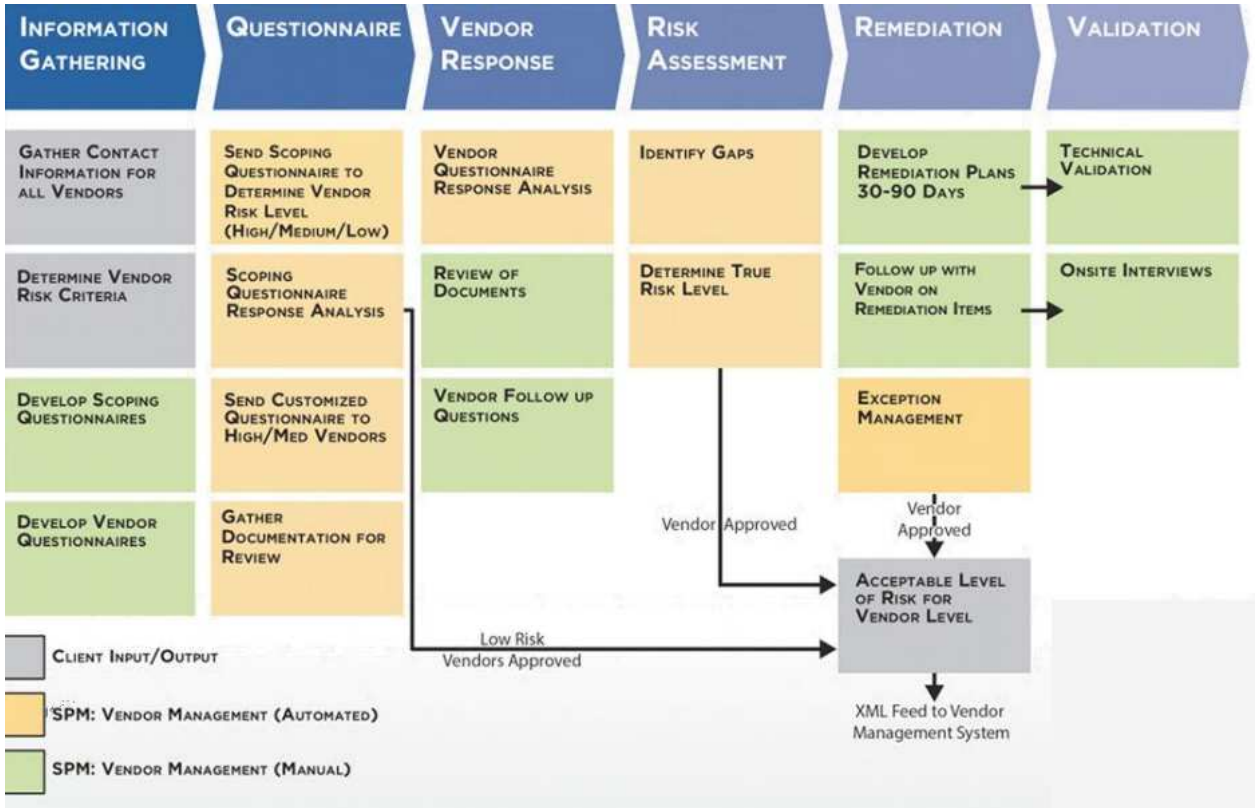
Evaluate designated physical security controls, including resilience and disaster recovery functions and the use of personnel and technology to prevent unauthorized physical access to critical assets.

- Examine change control management plans, including protocols on the installation of and execution of software.
- Assess the third-party vendor's system acquisition, development, and maintenance processes as it relates to the management of risks derived from software development and/or deployment of new software or hardware.
- Analyze incident response plans, including test plans and evidence of security incidents and lesson learned documentations required to maintain an integral chain of command.

Legal stipulations, within contractual provisions, which holds third-party service providers liable for cybersecurity incidents stemming from unmitigated vulnerabilities within their computing environment.

05 CONCLUSION

The measures described above—due-diligence, contractual terms, and continued monitoring and oversight—are critical elements of a comprehensive cybersecurity program as it relates to the management of third-party service provider relationships. To effectuate these elements, in turn, it is often helpful to have standardized processes and documentation. Examples of standardized processes and documentations include due-diligence checklists and questionnaires; template contract addendums addressing cybersecurity risk concerns; and standardized schedules for monitoring reviews and audits.



05 CONCLUSION

Third-Party Risk Management Procedure

Because there is no ‘one-size-fits-all’ approach that is appropriate for every third-party service provider, it is appropriate to implement a tiered approach that scales due-diligence, contractual obligations, and oversight processes according to the nature and extent of the cybersecurity risks presented by the business partnership. In all events, it is important that organizations periodically review their processes for evaluating and overseeing third-party relationships to ensure that such processes are up-to-date and appropriately tailored to address new and emerging cybersecurity threats.