Reducing Outsourcing Cyber Risks

By Paul A. Ashcroft, Ph.D., CPA

The scope of cyber risks is significantly expanding. Many firms utilize outsourced services to improve productivity and/or to reduce costs. Significant recent technological developments in the methods for delivering outsourced services have improved the capability and efficiency of the companies that provide such services.

However, the benefits from an increased use of outsourced services may be hampered by the correlating greater potential cyber risk vulnerabilities created for firms acquiring these services. Entities that acquire outsourcing services may be less than fully protected against these risks or perhaps unaware that they exist. The increase in outsourcing cyber risks provides CPAs with opportunities to develop and offer additional cyber risk advisory services.

Stan Lepeak, research director of KPMG's Shared Services and Outsourcing Advisory group, highlights items that significantly increase the risk of significant cyber-attacks for entities that extensively outsource their processes. Lepeak states that outsourcing creates opaqueness and uncertainty between the client and the outsource provider. He suggests avoiding the problems of the client not sufficiently understanding or having control over the provider's cyber protection procedures, and the provider not timely notifying the client when a breach does occur.

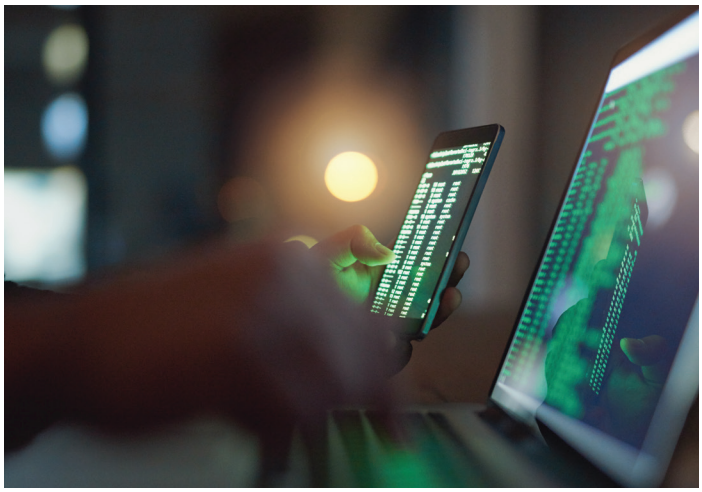
Indications of Significant Outsourcing Cyber Risks

Deloitte stated in their 2016 Global Outsourcing Survey that many companies today view outsource providers as key business innovators and enablers of transformation and not merely a cost-reducing option. This expansion of the outsourcer's role requires that companies allow outsourcers access to significantly more of a company's sensitive data, which increases the potential cyber risk exposure of data breach losses. Deloitte's survey reports that 73 percent of respondents consider cyber risks during the outsourcing process and that 23 percent expect to reduce their use of outsourcing in response to the related cyber risks.

Further indication of how outsourcing presents significant cyber risks to every organization is that Soha Systems reports that 63 percent of all data breaches result either directly or indirectly from access by third parties, such as outsourcing contractors and suppliers. Additional key results presented by Soha Systems in their 2016 Survey on Third Party Risk are:

- Organizations are providing third parties with increased access to their application infrastructure: 87 percent of IT professionals report that their organization's use of outsourcing contractors increased 49 percent since 2013 and 40 percent of the professionals expect it to continue increasing in the next three years.
- 56 percent of respondents were very concerned about their organization's ability to control and/or secure third-party access to their data.

Ponemon Institute conducts research on privacy, data protection and information security policy. Ponemon's 2016 survey of professionals



knowledgeable about proper governance of third party risks reports that responding organizations paid an average of $10 million over the previous 12 months to repair a data breach caused by negligent or malicious third parties. Regarding the extent of third party data risks, 21 percent of respondents replied they are significantly increasing, 20 percent said they are increasing and 29 percent stated the risks are not changing. Only 19 percent of respondents stated that their organization's third-party risk is decreasing and 11 percent said they could not determine the level of third party risks. Ponemon adds that 78 percent of their survey respondents expect the overall increasing trend in cyber-attacks to significantly impact their organization's third-party risk. In summary, the results of Ponemon's research provide additional indications of significant cyber risks from outsourcing.

The remainder of this article focuses on how entities can protect themselves against the cyber risks from outsourcing.

Initial Steps to Assess and Defend Against the Risks

Understanding the cyber risks a company may encounter from using outsourced services begins with asking clarifying questions. Business executives evaluating whether to increase their use of outsourced services would be wise to thoroughly answer these important cyber security questions:

- How is our company more vulnerable to cyber risk due to the technological changes in service delivery?
- How do we obtain the greater efficiency that results from an increased use of outsourced services and simultaneously reduce the correlating cyber risks to an acceptable level?

A major part of answering the above questions involves creating cyber security goals. Dan Kinsella and Steven Darroch of Deloitte & Touche recommend that firms develop and operate systems having the following three characteristics to effectively manage their service delivery cyber risks from outsourcing:

- Be secure: Protect critical assets against known and emerging threats;

Exhibit 1. Initial Defenses Against Outsourcing Cyber Risks

Defense	Key Actions
Be Secure	• Evaluate which data would cause the greatest disruption if it becomes unavailable and which data may be valuable to outsiders.
Be Vigilant and Resilient	• Fully include cyber security into the outsourcing procurement considerations. • Evaluate the effect of all outsourcing cyber security risks and issues on the overall business value chain. • Identify the specific controls and policies that should be implemented by the outsourcing supplier and require that each supplier fully and consistently follow them.

- Be vigilant: Reduce detection time and develop the ability to detect the unknown; and
- Be resilient: Strengthen your organization's ability to recover when an attacker makes it through your defenses.

Be Secure. Securing critical information to reduce cyber risks from outsourcing starts with identifying which types of data are the most critical and most valuable. Kinsella and Darroch state that executives should not think that their company's data is not valuable or not important merely because they have not experienced one of the high-profile data breaches that made national news. Rather, executives should thoroughly evaluate which data would cause the greatest disruption if it becomes unavailable, as well as which data may be valuable to outsiders. Cash flow and supply chain disruptions may result from important data becoming unavailable on a hosted or outsourced system.

Be Vigilant and Resilient. In the last few years, outsourcing has become a key strategy since one benefit of the increased use of a variety of supply chains is that it often eases entry into new markets. Whether outsourcing is for current markets or new ones, becoming more vigilant and resilient largely depends on implementing strong security controls.

In the majority of cases in which he has been directly involved, the controls required of outsourcing suppliers are "sadly lacking compared with those imposed on internal capabilities. And that is the soft underbelly that can expose a business to often difficult-to-manage cyber risk," states Mark Brown of Ernst and Young. Brown strongly advises the outsourcing buyer to:

- Fully include cyber security into their procurement considerations. Do not make financial savings the only goal of outsourcing.
- Evaluate the effect of all cyber security risks and issues on the overall business value chain. Do not merely assess cyber security from a technical perspective.

Security controls are critical, because a company's outsourcing of IT operations, supply and other business processes can create greater risks if cyber security standards are not equally and regularly followed by their contractors. Businesses can significantly reduce their risks by identifying the specific cyber security controls and policies that their suppliers should implement. In addition, the buyer should require each supplier to fully and consistently adhere to the specific controls and policies.

Exhibit 1 summarizes the key actions in developing important initial defenses against outsourcing cyber risks.

The High Cost of Cybercrime

According to Microsoft, the information security market totaled $170 billion in 2015, largely because 71 percent of companies reported having a 2014 cyber-attack and subsequently increased their security investments. Microsoft further stated that 556 million people are cybercrime victims annually. The World Economic Forum estimates the worldwide cost of cybercrime at $3 trillion.

Opportunity for CPAs

Companies acquiring outsourcing services should perform regular internal and/or external assessments to test the cyber security effectiveness of the vendor's systems. CPAs can provide needed assistance by conducting a Service Organization Controls 2 (SOC 2) review of the outsourcing vendor's system. A SOC 2 review is an attest engagement under the American Institute of CPAs' (AICPA's) Attestation Standards (AT) Section 101. AICPA's publication titled "Reports on Controls at a Service Organization over Security, Availability, Processing Integrity, Confidentiality or Privacy" provides specific guidance about performing a SOC 2 review.

AICPA states that a SOC 2 review report is intended to provide a broad variety of users with "information and assurance about the controls at a service organization that affect the security, availability and processing integrity of the systems the service organization uses to process users' data, and the confidentiality and privacy of the information processed by these systems." NDB LLP, Accountants and Consultants, explain that a SOC 2 review will examine and report on one or more of the "Trust Service Principles," which include the following:

- The security of a service organization's system.
- The availability of a service organization's system.
- The processing integrity of a service organization's system.
- The confidentiality of the information that the service organization's system processes or maintains for user entities.
- The privacy of personal information that the service organization collects, uses, retains, discloses and disposes of for user entities.

Due to the potentially high cyber risks of outsourcing, SOC 2 engagements provide CPAs with a valuable opportunity for adding services to current clients, as well as gaining new clients.

Reducing the Cyber Risks of Outsourcing

Cyber risks are continually present and cannot be totally eliminated. As such, it is very important to plan and implement effective procedures that reduce the risks associated with each outsourcing option considered. Buyers should perform each of the following procedures to reduce their outsourcing cyber risks, which are summarized in Exhibit 2 and are modified from recommendations by Brown and Lepeak.

1. Self-assessment. The firm acquiring the outsourcing services should thoroughly evaluate and understand their own level of

continued on next page

Exhibit 2. Specific Procedures to Reduce Outsourcing Cyber Risk

Procedure	Basic Description
Self-assessment	The buyer of outsourcing services thoroughly evaluates their own level of expertise and capability to defend against a cyber-attack.
Prioritize risks	Perform a holistic assessment of each supplier's data security tools and skills to identify where the significant risks are likely to occur.
Be employee cautious	Understand how the service provider trains and supervises its employees to handle, process and protect confidential information.
Involve experts	Have all of the client's internal experts and selected third-party experts assess the outsource provider's security methods and abilities.
Learn from mistakes	Study prior cyber-attacks on the client's organization and its peers, and determine how the provider learns from prior data security breaches.
Specify boundaries	The provider must notify the client of where its data resides at all times and may not sub-contract any of the delivery to another party.
Clarify controls	Clearly state to each outsourcer the information security, business continuity and privacy controls necessary.
Do a test run	Provide the supplier with a limited set of the company's data. Then test if the supplier has the desire and the ability to meet its obligations.
Be braced	Prepare for a cyber-attack by clearly predefining emergency and remedial response procedures for a variety of data breach scenarios.
Create a monitoring strategy	Monitor the supplier with continuous right-to-audit activities and the use of third-party testing beyond that of the outsourcing provider.
Observe intently	Observe in-depth the provider's response to early stage threats and attacks. Evaluate the quality and breadth of the provider's approach.
Plan for the possible consequences	Create a cyber-attack contingency plan and coordinate it with the outsourcer's contingency plan to reduce surprises and confusion.

expertise and capability to defend against a cyber-attack. This is needed to assess the quality of an outsourcing provider's defenses and define best practices that the provider should have in place and identify how to enforce those best practices.

2. Prioritize risks. In the planning/procurement stage, perform a thorough, holistic due diligence assessment of each supplier's data security tools, skills and abilities to identify where the significant risks are likely to occur. Avoid the mistake of focusing on just one area, such as network security, and skimming quickly over other areas such as data privacy and application security. While it is important to first protect the crown jewel assets, it is also vital to evaluate risks across all assets, applications and systems.

3. Be employee cautious. The outsourcer's employees will be handling and processing the client's data. Because of that, it is critical that the client fully understand and critique how the service provider trains and supervises its employees to handle, process and protect confidential information both internally and externally. For example, discover if employees handle sensitive data from different clients or store such data all in the same location on a common system. Also determine if the provider's employees possess all relevant and/or required training and certifications.

4. Involve experts. To accomplish a quality assessment of an outsource provider's data security methods, abilities and procedures, the client entity should involve all of their internal experts in the review process. Doing so will typically include many people beyond those who are specifically part of the team to acquire the outsourcing services. If the client's personnel lack critical knowledge or skills to properly perform portions of the assessment, it is vital to contract with third-party experts to overcome those weaknesses. The outsourcing provider should also have skilled security experts already in place.

5. Learn from mistakes. Identify the types of attacks that may occur and possible controls to prevent them by studying actual cyber-attacks that the client's organization and its peers have experienced. In addition, determine if the provider is taking a similar approach to learn from prior data security breaches. From this entire process, the client and the outsource provider should then collaborate to clearly define and agree on leading practices to reduce the cyber risks appropriately.

6. Specify boundaries. The client organization should require that the outsource provider notify them of where its data resides at all times and that the client retains the right to not allow the data to be moved out of agreed-upon markets. In addition, impose on each supplier sufficient restrictions that prevent the outsourcer from sub-contracting any of the delivery to another party. This is vital in order to pinpoint responsibility.

7. Clarify controls. State clearly in the contract with each outsourcer the information security, business continuity and privacy controls necessary to comply with the company's internal policies, as well as laws and regulations.

8. Do a test run. Prior to transferring full responsibility to the supplier, provide the supplier with limited access to a set of the company's data. Then perform acceptance testing to assess if the supplier has both the desire and the ability to fulfill its contractual obligations.

9. Be braced. Prepare in advance that a significant cyber-attack will hit the firm and its provider at some future time. Right now, clearly predefine emergency and remedial response procedures for a variety of data breach scenarios.

10. Create a monitoring strategy. After fully transferring data responsibility to the supplier, do not become complacent that the outsourcing provider is maintaining adequate cyber-attack defenses. Reduce long-term cyber risk in the supply chain by closely monitoring the supplier with continuous right-to-audit activities, such as network penetration and applicable vulnerability testing. Consider the use of third-party testing beyond that of the outsourcing provider, for example via the use of "ethical" hackers. Thoroughly review the provider's data defense strategies, tools and risk environment on a frequent and regular basis. Pay very careful attention to the connection points between the systems and applications used by the outsource provider.

11. Observe intently. In a careful, focused, detailed manner, observe how the provider responds to threats and early stage attacks.

DON'T MISS: TSCPA'S 2018 TEXAS CPA TECHNOLOGY CONFERENCE ON MAY 7-8 IN ADDISON OR MAY 10-11 IN HOUSTON. FOR MORE INFORMATION AND TO REGISTER, VISIT THE CPE SECTION OF OUR WEBSITE AT TSCPA.ORG.

Have the client's executives and security experts evaluate how comfortable they are with the quality and comprehensiveness of the provider's approach. Quality of the response is much more important than speed, because a rushed reaction to an attack can provide the perpetrator with additional vital information about the organization and its defenses. If the client considers the provider's methods to be inadequate, insist that the provider install proper methods within a limited time, such as 10 to 15 days, or the client will find another provider.

12. Plan for the possible consequences. Since preventing all cyber-attacks is impossible, the client should create a cyber-attack contingency plan in advance and compare/coordinate their plan with the outsourcer's contingency plan. In the event of an attack, it is essential to fully understand the consequences on the firm and its obligations as compared to those of the outsource provider. Having a clear contingency plan and an understanding of the provider's contingency plan should significantly reduce the number of unexpected surprises and potential confusion about each entity's responsibilities, which is very valuable in the already stressful event of a cyber-attack.

Make a Comprehensive Plan

Outsourcing typically provides significant cost reductions and efficiency improvements. However, companies acquiring such services are advised to thoroughly assess the cyber risks involved in acquiring these services.

Proper overall management of cyber risks requires selecting a reliable and diligent supplier of outsourcing services. Selecting outsourcers of lower quality may result in significant cyber-security breaches that could have been rather easily prevented.

This article presented several specific methods to reduce the cyber risks of outsourcing. The foundation of these methods are identifying which data is most valuable, holistically assessing the outsource provider's ability to implement and adhere to proper controls over confidential information, learning from prior cyber-attacks, and performing regular and detailed monitoring of the provider by using continuous right-to-audit activities and third-party testing.

In particular, CPAs can perform a SOC 2 review that reports on the security and integrity of the vendor's systems processing the client's data. ■

References

AICPA. *Service Organization Controls (SOC) Reports for Service Organizations*, www.aicpa.org/interestareas/frc/ assuranceadvisoryservices/pages/serviceorganization'smanagement.aspx.

Brown, Mark. October 2013. "Outsourcing: The soft underbelly of cyber risks," *Computer Weekly.* www.computerweekly.com/opinion/Outsourcing-the-soft-underbelly-of-cyber-risks.

Deloitte Touche Tohmatsu Limited. 2016. *Global Outsourcing Survey 2016.* www2.deloitte.com/us/en/pages/operations/articles/global-outsourcing-survey.html.

Kinsella, Dan and Steven Darroch. Nov. 1, 2016. *Cyber risk management in service delivery transformation,* Deloitte & Touche LLP. www2.deloitte.com/us/en/pages/ operations/articles/cyber-risk-management-in-service-delivery-transformation.html.

Lepeak, Stan. Oct. 24, 2012. "Cyber Attacks and Outsourcing: Prepare for the Worst, While Hope for the Slightly Bad," *Nearshore Americas.* www.nearshoreamericas.com/cyber-attacks-outsourcing-risk/.

Microsoft Secure Blog Staff. Jan. 27, 2016. *The Emerging Era of Cyber Defense and Cybercrime.* Microsoft Inc. http://blogs.microsoft.com/microsoftsecure/2016/01/27/the-emerging-era-of-cyber-defense-and-cybercrime/.

NDB LLP, Accountants and Consultants. *SOC 2 Reporting Framework and the Top 10 Items You Need to Know About.* https://socreports.com/white-papers/soc-2-reporting-framework-essentials-part-i.html.

Ponemon Institute. May 2016. *Tone at the Top and Third Party Risk.* https://media.scmagazine. com/documents/229/ponemon-report-final_%281%29_57220.pdf.

Soha Systems. 2016. *Survey on Third Party Risk Management.* Soha Sytems Inc., http://go.soha.io/hubfs/Survey_Reports/Soha_Systems_Third_Party_Advisory_Group_2016_IT_Survey_Report.pdf?t=1467123126371

Paul A. Ashcroft, Ph.D., CPA is an associate professor in the School of Accountancy at Missouri State University, where he teaches auditing, advanced auditing and intermediate accounting. He has published articles in several journals, including *Today's CPA, International Journal of Critical Accounting, Advances in Accounting, Incorporating Advances in International Accounting, Research in Accounting Regulation, The CPA Journal, the Oil, Gas and Energy Quarterly* and *Internal Auditing.* He currently serves on the editorial review board of *The International Journal of Accounting, Auditing and Performance Evaluation.* He is a member of the American Accounting Association and the Institute of Internal Auditors. Contact him at paulashcroft@missouristate.edu.