THIRD-PARTY RISK: SECURING THE MODERN COMPLEX BUSINESS

KEY ISSUE:

Risks from third parties create security unknowns

The risks third parties pose to enterprises continue to mount, even as security leaders accelerate their efforts to improve overall security. As CISOs improve network, endpoint, application and user-level security, third parties are becoming the entry points to some of the largest breaches to date.

- The most public example of this type of breach is the retailer behemoth Target. Target experienced a near-catastrophic breach of their payment card platform and network through a third party HVAC company.[1] Target's HVAC provider, Fazio Mechanical, suffered a compromise. Attackers used stolen credentials to access Target's network and perform a compromise of their payment card network and systems. Even though steps were being taken to improve Target's security presence internally, this breach of a third party was a catalyst for one of the largest, and most expensive, data breaches to date.

As significant as this third party breach was, Target is just one of many. Other examples include:

- T-Mobile recently announced that Experian, whom T-Mobile uses to perform credit checks for potential customers, was breached and lost the records of 15 million people.[2]
- Retailer Goodwill suffered a third party breach involving their payment processor that exposed nearly 900,000 credit card records. Forensic investigations revealed that the third party vendor's systems had been compromised by malware providing attackers with access to credit card data for over a year between February 2013 and August 2014.[3]
- In September 2011, the U.S. Defense Department's TRICARE health program notified 4.9 million beneficiaries of a data breach; the breach occurred when backup tapes were stolen from the car of an employee of Science Applications International Corp., one of TRICARE's business associates.[4]

CHALLENGES AND OPPORTUNITIES:

Handling Third-Party Risk Starts with Awareness

The inter-dependency of connected systems and business relationships requires a strong third party risk plan that extends beyond traditional IT. Third party risk may start with a focus on network interconnects and data exchanges, but ultimately the challenge becomes bigger than just IT. As organizations mature, initial focus should be given to relationship risk – the nature of the third party relationship; but also to business profile risk – the inherent risk of the business profile of the third party. The initial ownership of this evolution starts with the CISO and an understanding of connectedness and data.

One of the key topics of discussion is the attempt by some companies to shift liability of an external breach to a third party. Even though this may be accomplished through legal documents on paper, customers are more likely to hold the company they entrust with their data accountable than the contracted third party. This issue is still far from settled, and there is much legal precedent to be had here. Additionally, a single third party breach will likely impact multiple enterprise partners and thus significantly amplify difficulties in cleaning up the fallout.

- Roughly 63 percent of breaches come from third parties.[5]

As a result of the third party relationship, during a breach situation:

- Incident management is orders of magnitude more complex
- Incident response is significantly slower
- Costs of response and remediation, including legal costs, are significantly higher

Additionally, due to the issue being with a third party, there is little or no control over breach disclosure timeliness, messaging and public relations, legal or regulatory aspects.

THE PATH FORWARD:

Develop a Focused Program Strategy

Enterprise security should take this opportunity to be a business enabler. By gaining understanding of business-critical data and business processes, security teams have an opportunity to lay the foundation of a sound third party risk program. Enterprise security can lead the conversation, beginning with the basics like sensitive data exchange and network inter-connects, then developing a strategy forward.

The role of the Enterprise Security Executive is critical here as the technology executive taking on the challenge of helping the business manage risk in a meaningful fashion. As the CISO's role in the enterprise continues to evolve and take shape, this is a prime opportunity to gain visibility in a positive manner. The CISO has an opportunity to elevate their role beyond the traditional technologist and into a broader enterprise risk context.

Sound strategy starts with a clear definition of what third party risk means to the organization. An enterprise-wide program must involve key stakeholders from legal, enterprise risk and other business critical functions in order to be successful and adopted across the business. By focusing the third party risk program on achievable key outcomes and backing them with clear key performance indicators (KPIs), the program becomes part of enterprise due-diligence and can support the collection of evidence when needed.

A. *Address the key components of third party risk*

- Third parties can be understood as having two major components:
  - » Relationship risk – the inherent risk that arises from the business relationship. For example: exchanging social security numbers with a third party to perform a credit check.
  - » Business profile risk – the inherent risk that is present from the nature of the third party business. For example: business profile risk may be based off a Dun & Bradstreet DUNS number lookup to understand the company's creditworthiness and other attributes.
- There are seven key types of third party risk that must be addressed:
  - » Strategic – adverse long-term business impact
  - » Reputational – negative public opinion
  - » Operational – failed internal processes, people or systems
  - » Transactional – problems with product or service delivery
  - » Financial – inability to meet contractual/ financial obligations
  - » Compliance – violation of applicable laws, regulations
  - » Foreign – country, culture, geopolitical or foreign currency

B. ***Focus on scope, assessment methodology, remediation capabilities***

As the enterprise security organization seeks to build and define a third party risk program, leaders should focus on the three most critical components. Setting clear objectives for the scope, assessment methodology and remediation capabilities allows the organization to have well-defined and achievable goals.

Scope will broaden as the program matures and capabilities develop. Organizations should initially focus on the things that are within the scope of enterprise security: data and network handoffs. Wherever data is being handed off (electronically) to a third party, there is an opportunity to identify these third parties and assess the process. Additionally, network interconnectivity points are crucial and can provide audit hooks to define a standardized model for third party access.

Assessment methodology will mature over the program's life as well. Initial focus should center on a simple self-assessment questionnaire written to maximize information collection from third parties, and eventually grow into a multi-pronged approach. This latter approach should leverage a risk-tiered strategy, one-on-one discussions, on-site assessments and tools – allowing the third party risk program to expand its ability to assess risk in lock-step with the scope.

Remediation is tricky primarily because the security organization doesn't always have the ability to influence change directly. Initial focus should be on providing guidance back to the internal business stakeholders, and then to the affected third party; over time, the program should evolve to establish a bi-directional protocol for active feedback and continuous re-assessment mutually benefitting both parties.

C. ***Define and Appropriately Measure Success***

The hallmark of a strong program is being able to quantitatively and qualitatively define its current position. Defining goals and measurements – with a strong focus on business alignment – is just as important as demonstrating program advancement. Without having business-aligned targets to execute against, it is impossible to understand whether the third party risk program is advancing the goals of the enterprise or not.

The KPI set must have meaning to the enterprise and not simply be an aggregate of numbers on a spreadsheet. Measuring how many third party assessments were completed in a given quarter holds significantly less meaning than demonstrating the percentage of enterprise critical relationships that have been successfully driven through a vetting process. Both of these measurements have meaning, but only the second one has significance to the broader business.

As the program matures, it should be expected that KPIs produced by the third party-risk program would be used to identify leading and lagging program participants and help drive consideration as contract negotiations come due. For example, continuing a relationship with a lower cost, but high-risk third party that consistently fails to remediate identified risks may not be in the company's best interest. Especially if a competitor does a better job and demonstrates a higher level of due care. The second relationship may seem more expensive in terms of contract dollars, but the level of real risk reduction should provide input to the value equation.

CALL TO ACTION:

Businesses have always had third parties, and thereby, third party risk. However, the explosion in digital interconnectedness and resulting complexity of business relationships means a dramatic increase in the threat landscape. As companies take on more relationships and connect to more third parties – these risks drive up the number of unknowns for security. Security doesn't like unknowns.

A strong third party risk program is a must for any enterprise security organization and an opportunity for the CISO. Even though building such a program necessarily requires board-level visibility, accountability and ownership, the CISO's role is pivotal to successful execution. Now is the time for the CISO to truly become a business enabler; the steps required to define, operationalize and drive a strong third party risk program originate in enterprise security. The CISO can do this by focusing on achievable, business-aligned goals, setting maturity milestones, and measuring outcomes.

1 Lemos, Robert. "Target Breach Underscores Need to Monitor Third party Network Access" eWeek. February 6th, 2014. Retrieved from: http://www.eweek.com/security/target-breach-underscores-need-to-monitor-third party-network-access.html

2 Legere, John. "T-Mobile CEO on Experian's Data Breach" T-Mobile. October 2015. Retrieved from: http://www.t-mobile.com/landing/experian-data-breach.html

3 Goldman, Jeff. "Goodwill Data Breach Linked to Third Party Vendor" eSecurity Planet, September 2014 Retrieved from: http://www.esecurityplanet.com/network-security/goodwill-data-breach-linked-to-third party-vendor.html

4 "Third party Service Providers (TSPs) Breach Impact & Preparedness" Bank Info Security.com. 2012. Retrieved from: http://www.bankinfosecurity.com/webinars/risk-management-third party-breach-impact-preparedness-w-289

5 Ashford, Warwick. "Bad Outsourcing Decisions Cause 63% of Data Breaches" Computer Weekly.com February 2013. Retrieved from: http://www.computerweekly.com/news/2240178104/Bad-outsourcing-decisions-cause-63-of-data-breaches

1125 17th Street, Suite 1700
Denver, CO 80202

800.574.0896 | www.optiv.com

Optiv is the largest holistic pure-play cyber security solutions provider in North America. The company's diverse and talented employees are committed to helping businesses, governments and educational institutions plan, build and run successful security programs through the right combination of products, services and solutions related to security program strategy, enterprise risk and consulting, threat and vulnerability management, enterprise incident management, security architecture and implementation, training, identity and access management, and managed security. Created in 2015 as a result of the Accuvant and FishNet Security merger, Optiv is a Blackstone (NYSE: BX) portfolio company that has served more than 12,000 clients of various sizes across multiple industries, offers an extensive geographic footprint, and has premium partnerships with more than 300 of the leading security product manufacturers. For more information, please visit www.optiv.com.

11.15 | F1