RISKALERT™ 2019-2

61% of US Organizations Experienced Data Breach Due to 3rd Parties in 2017

By Don McConnell
CIPP/US
RiskSmart Advisors
January 16, 2019

The Ponemon Institute recently released its ***Data Risk in the Third-Party Ecosystem: Third Annual Report*** which emphasizes the critical need for organizations to up their efforts when managing their 3rd Party Ecosystem (3PE)[1] risk. The report reveals the challenges organizations continue to face as they try to protect the sensitive and confidential information shared with third parties and their third parties (Nth party risk) at a time when reliance on 3PEs continues to grow.

> *"Considering the explosive growth of outsourced technology services and the rising the volume of third parties, companies need to take control of their third-party exposure and implement safeguards and processes to reduce their vulnerability"*
>
> Dr. Larry Ponemon[2]

The 3PE Risk

Some highlights from the report illustrate the extent of 3PE breaches and the lack of managing basic 3PE risks:

1. 61% of US organizations experienced a data breach caused by a third party or vendor, a 5% annual increase;

[1]The report defines "3rd Party Ecosystem" as the many direct and indirect relationships companies have with third parties and Nth parties.

[2] AP News. Opus & Ponemon Institute Announce Results of 2018 Third-Party Data Risk Study: 59% of Companies Experienced a Third-Party Data Breach, Yet Only 16% Say They Effectively Mitigate Third-Party Risks. November 15, 2018

2. Companies shared confidential and sensitive information with around **583 third parties**, on average;
3. Only **34%** keep a comprehensive inventory of those parties;
4. Only **15%** know how their information is being accessed or processed by Nth parties.

Many 3PE businesses are small/midsized businesses (SMB) and those businesses continue to be primary focus for the cyber criminals.

> *"Small and midsize businesses are not just targets of cybercrime; they are its principal target"*
>
> Commissioner Luis A. Aguilar, U.S. Securities and Exchange Commission[3]

However, most SMB's don't think they are at risk.

> "*As a result, it's fair to say they are indeed ill-prepared to safeguard against an attack*"
>
> Bryan Seely, a network engineer famous for hacking into the FBI[4]

And the criminals know they are ill-prepared. When you consider the growth in reliance on 3PEs, the findings of the Ponemon report and the observations from above you can see the incredible threat of 3PE risk.

Regulators and 3PE Risk

3PE risk management pressure from regulators continues to increase. The Federal Trade Commission (FTC) is viewed as the leading regulator on data security in the US. The FTC expects a business to ask vendors detailed questions about their data security practices **before** any information is shared. The Health and Human Services Office of Civil Rights has the same expectations. The New Jersey Attorney General made the following statement in an enforcement action from last year:

> "*Having a good handle on your own cybersecurity is not enough. You must fully vet your vendors.*"[5]

[3] The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses.
[4] CNBC, Congress addresses cyberwar on small business: 14 million hacked over last 12 months
[5] Press Release, New Jersey Division of Consumer Affairs, April 4, 2018

The mitigation of these risks has become even more important with the EU's General Data Protection Regulation and the California Privacy Act. Regulators read reports like the Ponemon report, they see what the issues are and what reports like this identifies as "best practices."

3PE Best Practices

The Ponemon report includes a special analysis of those organizations that have been able to avoid a 3PE breach in the past 12 months or ever. The report found those organizations engage in the following best practices:

1. **Evaluation of the security and privacy practices of all third parties.** In addition to contractual agreements, conduct audits and assessments to evaluate the security and privacy practices of third parties.

2. **An inventory of all third parties with whom you share information.** Create an inventory of third parties who have access to confidential information and how many of these third parties are sharing this data with one or more of their contractors.

3. **Frequent review of third-party management policies**. The third-party risk management committee should create a formal process for and regularly review the security and privacy practices of their third and Nth parties to ensure they address new and emerging threats, such as unsecured Internet of Things devices.

4. **Third party notification when data is shared with Nth parties**. Companies should include in their vendor contract requirements that third parties provide information about possible third-party relationships with whom they will be sharing sensitive information.

5. **Oversight by the board of directors**. Involve senior leadership and boards of directors in third-party risk management programs. This includes regular reports on the effectiveness of these programs based on the assessment, management and monitoring of third-party security practices and policies. Such high-level attention to third-party risk may increase the budget available to address these threats to sensitive and confidential information.

6. **Visibility into third or Nth parties with whom you do not have a direct relationship.** Increase visibility into the security practices of all parties with access to company sensitive information – even subcontractors.

7. **Accountability for proper handling of third-party risk management program.** Centralize and assign accountability for the correct handling of your company's third-party risk management program and ensure that appropriate privacy and security language is included in all vendor contracts.

3PE Risk Management is a Process

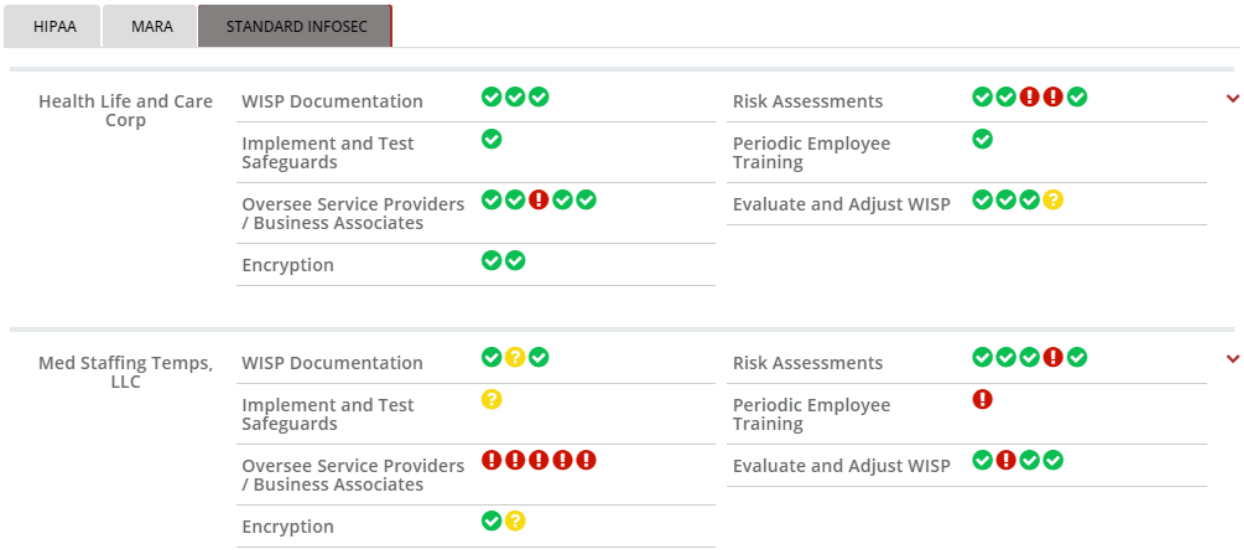
"*Data security is a journey, not an end point.*"

Maneesha Mithal
Associate Director, FTC

3PE risk management is part of that data security journey. Your information program needs risk-based processes in place to identify and manage your evolving 3PE risks.

We can help you with your data security processes including managing 3PE risks.

Our RiskPortal provides you with the process framework that allows you to intelligently and proactively identify 3PE risk challenges and regulatory demands your business faces. We track, analyze and adjust our solutions to account for the latest developments in



InfoSec laws and regulations. With RiskSmart's InfoSec risk management solutions and processes you create, maintain and manage a fundamentally sound written information security program, all delivered digitally through our RiskPortal in a cost effective and efficient manner.

Our **WISP Dashboard** gives you easy and instant visualization of your information security program, including managing your 3PE risks.

If you have questions about these InfoSec compliance issues please feel free to e-mail us at compliance@risksmartadvisors.com.

About RiskSmart Advisors, LLC

Founded in 2015 **RiskSmart Advisors, LLC** (RSA) is a leading information security risk management software service provider. RSA develops unique InfoSec risk management tools leveraging a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about RSA InfoSec solutions for enterprise line of business users and SMBs at www.risksmartadvisors.com.

Corporate Headquarters:
1650 West End Blvd, Suite 100
St. Louis Park, MN 55416
Phone: +1 844.637.5511
Fax: +1 763.251.0356
www.risksmartadvisors.com