8 Steps to Protect against Rising Third Party Cyber Risks

– Anil Lamba
Practice Lead - Cyber Security, EXL Service Inc., NJ, USA
https://orcid.org/0000-0002-7793-785X dranillamba@outlook.com

Article History
Paper Nomenclature: Column (CLM)
Paper Code: CYBNMV1N5OCT2019CLM1
Submission Online: 02-Oct-2019
Manuscript Acknowledged: 08-Oct-2019
Originality Check: 10-Oct-2019
Originality Test Ratio: 4%
Peer Reviewers Comment: 18-Oct-2019
Blind Reviewers Remarks 19-Oct-2019
Author Revert: 20-Oct-2019
Camera-Ready-Copy: 22-Oct-2019
Editorial Board Citation: 27-Oct-2019
Published Online First: 31-Dec-2019

Third parties are often your weakest link making you vulnerable to data breaches.So, it's becoming very clear that you need strong processes in place to protect your organization from third party cyber risk

Keywords : Cyber | Data Privacy

Introduction:

Here are 8 key steps to protect against third-party cyber risks:-

1. **Have dedicated resources -** Employ experts internally that understand how to assess and monitor a vendor for cybersecurity preparedness and risks. We recommend a CISSP (Certified Information Systems Security Professional) or someone with many years of IT experience. In addition, make sure they have the tools available to appropriately monitor the risk and time to allot to these tasks. If you don't have the capacity to have a resource on staff, then consider outsourcing to a third party expert.

2. **Include cybersecurity in your organization's third party risk management scope -**Consider vendor cyber risk when planning your vendor management goals for the upcoming year. This helps enable you to mitigate risk by allowing you to influence the vendor to strengthen their controls, supplement their controls with your own and make a decision on whether you should stay with that vendor. It's imperative that you demonstrate you are taking proactive steps to identify and mitigate potential areas of weakness with your vendors.

3. **Write cybersecurity due diligence into your program -** Ensure it's included as a requirement in your program, as well as in your exam preparation. Due diligence should include a risk assessment that addresses cybersecurity concerns.

4. **Understand the inherent risk present -**Organizations must solidify a methodology to identify the inherent risk from cyber threats at their vendors – before a cyber risk occurs.

5. **We recommend you review the following four cybersecurity related areas for your vendors:**

- **Security Testing -** Testing should always be included in your vendor's program scope. It's a great way to identify weaknesses.
- **Sensitive Data Security -** Verify that your vendor can protect information against unintended disclosure by protecting it from destructive forces, such as data breaches, and unwanted actions of unauthorized users.
- **Employee, Contractor and Vendor Management -** Your vendor should be able to verify that their employees, contractors and vendors (your fourth parties) are trained and prepared to protect data.
- **Incident Detection and Response -** An incident is anything that impacts the confidentiality, integrity or availability of information or an information system. Your vendor should have a plan to address incidents effectively and quickly.

1. **Ensure your vendor's cybersecurity program aligns with your organization's program -** When looking at your vendor's cybersecurity posture, you should:

- **Identify** the threats your vendor could present and proactively mitigate potential areas of weakness.
- **Determine** if your vendor and any customer data they have access to will be secure.
- **Review** if your vendor is prepared to address a cybersecurity issue or event.

2. Request a SOC for Cybersecurity as needed **-** The American Institute of Certified Public Accountants (AICPA) released guidance relating to a cybersecurity risk management reporting framework on April 26, 2017. It provides a common language for vendors to use in describing their cybersecurity risk management program effectiveness. This is a helpful report for you to compare vendors.

3. **Prepare Controls - Once your team identifies any inherent risk present, document it and prepare to mitigate the risk. Here are a few ways to do so, per the FFIEC guidance:**

- **Risk Management and Oversight -** Involves governance, allocation of resources as well as training and awareness of employees.
- **Threat Intelligence and Collaboration -** The acquisition and analysis of information to identify, track and predict cyber capabilities, intentions and activities that offer courses of action to enhance decision making.
- **Cybersecurity Controls -** Controls can be preventive, detective or corrective.
- **External Dependency Management -** Includes the connectivity to third party service providers, business partners, customers or others and the organizations' expectations and practices to oversee these relationships.
- **Cyber Incident Management and Resilience -** Involves incident detection, response, mitigation, escalation, reporting and resilience.

Dr Anil Iamba is a notable industry speaker, researcher, an innovator, and an influencer with proven success in spearheading Strategic Information Security Initiativesand Large-scale IT Infrastructure projects across industry verticals. He is Ph.D. Cyber Security, CISA ® and hold various other impressive industry credentials. He has helped bring about a profound shift in cybersecurity defense.

Anil leverages his skills and pervasive industry experience to help customers understand risks in their systems and develops programs to mitigate those risks. He has also volunteered himself to act as a cybersecurity adviser for undergraduate college students in the U.S. conducting independent researches.

dranillamba@outlook.com

Annexure I

Submission Date	Submission Id	Word Count	Character Count
02-Oct-2019	1177376320 (Turnitin)	1556	9038

ORIGINALITY REPORT

4%	%	4%	%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	José María Blanco, Jéssica Cohen, Holger Nitsch. "Chapter 5 Cyber Intelligence Against Radicalisation and Violent Extremism", Springer Science and Business Media LLC, 2020 Publication	4%

Note: www.Cybernomics.in Uses a "Turnitin" https://www.turnitin.com which is an American commercial, Internet-based plagiarism detection service, a subsidiary of Advance and also offers plagiarism-detection service for newspaper editors and book and magazine publishers called iThenticate..

Reviewers Comment

Reviewer Comment 1: Some of the biggest cyber threats stem from the move to new technologies, like the Internet of Things (IoT). As networks disperse and more devices develop greater connectivity, security measures will have to evolve, too. Here are a few common reasons businesses fall victim to cyber attacks:

Reviewer Comment 2: This article bonafidely describes some steps to protect from cyber crimes…

Some important steps are

- Have dedicated resources
- Understand the inherent risk present
- Ensure your vendor's cybersecurity program aligns with your organization's program

Reviewer Comment 3: Cyber risk is any risk associated with financial loss, disruption to operations or damage to an organisation's reputation from a negative event impacting the organisation's information and/or information systems.

Editorial Excerpt

The article has 4% of plagiarism which is accepted percentage for publication The finding related to this manuscript is vital and into "8 Steps to Protect Against Rising Third Party Cyber Risks" Cyber risk commonly refers to any risk of financial loss, disruption or damage to the reputation of an organization resulting from the failure of its information technology systems. Cyber risk could materialize in a variety of ways, such as:

- Deliberate and unauthorized breaches of security to gain access to information systems.
- Unintentional or accidental breaches of security.
- Operational IT risks due to factors such as poor system integrity.

The article has been earmarked to and finalize to be published under the category of "**Column**"

Scholastic Seed Inc.
www.scholasticseed.in

Citation

Anil Lamba
"8 Steps to Protect Against Rising Third Party Cyber Risks"
Volume-1, Issue-5, Oct 2019. (www.cybernomics.in)

Frequency: Monthly, Published: 2019
Conflict of Interest: Author of a Paper had no conflict neither financially nor academically.