Common Flaws that Create Risk Through Third Party (Program) Risk Management
# Table of Contents

1. What is the problem?  
   Third party risk management programs may create increased cyber risk

2. What are the flaws?  
   There are common flaws to look for when assessing your potential third party risk management vendor

3. What are the solutions?  
   How do you protect your third-party risk management program?
David Mayer

*Dave* is the CIO and Managing Director of Advanced Assessment at Neuvik. He is responsible for end-to-end Red Team engagements, network penetration testing, web apps assessments, and more. He has been the offensive Red Team director for technical consulting firms as well as a member of the Red Team at Citibank.

**Certifications:** GIAC GSE, GSEC, GSNA, GCIA, GCFE, GPEN, GXPN, GCIH, GWAPT, GAWN, OSCP
Where is the problem?
Third Party Risk Management (TRPM) is an essential component of any organizational cybersecurity risk management program. TPRM programs help identify and mitigate risks to your organization introduced by external parties, ultimately trying to achieve the reduction of cyber risk provided by third parties.

What is third party risk management?
What are the common flaws?
So, what flaws keep coming up?

What is the irony of assessing your third party for third-party risk?

Flaws may exist in externally used vendor risk systems, and these flaws can act as the perfect map for attackers to discern which vendors do business with which companies; just imagine what this might look like for your organization.

Insecure Applications

1. Lack of role-based access. The lack of role-based access allows unauthorized users to gain access to data ripe for a third-party attack. Many times, we see this in antiquated applications that simply do not allow role-based authentication.

2. Lack of secure development. Insecure code provides countless classes of attacks by unauthorized users. Many times, applications are pushed to production without proper security reviews, leaving insecure code in production applications used by third-party risk management vendors.

Insecure File Transfer

Transferring files without proper security also provides opportunities for an unauthorized user. Many times, we see a practice of direct unencrypted emailing of sensitive information during risk questionnaires, or TPRM due diligence.
The insecure application: Lack of role based access control

*The scenario:* In the case of one vendor, we were able to gain access to tax and bank account information for every third-party that had been in contact with any of the hundreds of organizations using the platform. We achieved this by using an old (circa-2000) attack of forcibly browsing — simply changing, or guessing, the URL, to move up a directory level. Once there, access to unauthorized data was achievable.
All vendors for the platform
All clients for the platform
Vendor Banking Information

June 1, 2021

IMPORTANT | Transaction Routing Instructions (ACH and Wire)

Dear [Redacted],

Thank you for your request for account and bank routing number information for [Redacted]

Please provide the below routing instructions for ACH and wire transactions to remitters who send transactions to the company account.

For accurate and timely processing of transactions, it is very important that remitters correctly identify the company account number and the applicable routing number.

For ACH delivery:
Bank Routing Number:
Account Number:
Account Name:

For Wire Transfers:
Bank Routing Number:
SWIFT Code:
General Bank Reference Address:
Account Number:
Account Name:

We are here to help.
Please call me if you have any questions. Thank you for your business and the opportunity to serve you.
# Vendor W9 Information

## Request for Taxpayer Identification Number and Certification

**Form W-9**

**Department of the Treasury Internal Revenue Service**

### Part I: Taxpayer Identification Number (TIN)

- **Social security number**
- **Employer Identification number**

### Part II: Certification

- Under penalties of perjury, I certify that:
  1. I have filled out the form accurately and completely.
  2. The information provided is true and correct to the best of my knowledge.
  3. I am not subject to backup withholding because: (a) I am not required to file a tax return, (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding.
  4. The FATCA code(s) entered on this form indicate that I am exempt from FATCA reporting.

**Certification instructions:** You must cross out item 2 above if you have been notified by the IRS that you are subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and certain tax-exempt interest, other than interest and dividends, you must complete Form W-9 and attach it to your tax return. If you have questions about an item, contact the IRS at 1-800-829-1040.
The insecure application: Lack of secure development

**The scenario:** In several software providers, for example, we found debug functionality left “enabled,” allowing for the enumeration of the system, running processes and memory. We were also able to discover client-side controls for administrative access, where an unauthorized user may change a 0 to 1 in the JavaScript to enable the administrative functionality on a given page.
The insecure file transfer

The scenario: Too many organizations still request information by unencrypted email, providing the opportunity of sensitive information remaining on the servers. Even though encryption may be an option when received, the information may remain unencrypted on the servers on the receiving end. The use of a secure file sharing platform to reliably and securely transfer sensitive information can simply solve for this security flaw.

The organization requested the following information:

- Full copies of company policies
- Firewall configurations
- Number of system administrators, and their names
- All DLP rules and their configuration
- Copy of the asset inventory
- Content filtering configuration
- All Administrative Access processes and procedures
Things are getting interesting
### Things are getting interesting

<table>
<thead>
<tr>
<th>Environment</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java VM</td>
<td>1.7</td>
</tr>
<tr>
<td>Java Platform API Specification</td>
<td>Oracle Corporation</td>
</tr>
<tr>
<td>Java VM Specification</td>
<td>1.7</td>
</tr>
<tr>
<td>Java VM Vendor</td>
<td>Oracle Corporation</td>
</tr>
<tr>
<td>Java VM Version</td>
<td>24.291-b09</td>
</tr>
<tr>
<td>Java Management Builder Initial</td>
<td>Weblogic management jmx.mbeanserver.WLSBeanServerBuilder</td>
</tr>
<tr>
<td>Java XML CORBA, PortableRemoteObjectClass</td>
<td>Weblogic.topology.PortableRemoteObjectDelegateImpl</td>
</tr>
<tr>
<td>Java XML CORBA, UI Class</td>
<td>Weblogic.topology.PortableRemoteObjectDelegateImpl</td>
</tr>
<tr>
<td>Java XML Parsing DocumentBuilderFactory</td>
<td>Oracle.xml.jaxp.JDOMDOCUMENTBuilderFactory</td>
</tr>
<tr>
<td>Java XML RPC Service Factory</td>
<td>Oracle.xml.soap.DocumentBuilderFactory</td>
</tr>
<tr>
<td>Java XML SOAP Message Factory</td>
<td>Weblogic.soap.MessageFactoryImpl</td>
</tr>
<tr>
<td>JBO 323 Compatible</td>
<td>true</td>
</tr>
<tr>
<td>JRE Version</td>
<td>1.1.1</td>
</tr>
<tr>
<td>Jaxb paxos</td>
<td>/u003/app/appmgr</td>
</tr>
<tr>
<td>Java VM Exe</td>
<td>/u003/app/appmgr</td>
</tr>
<tr>
<td>Oracle Apmaas Agent Root Config Dir</td>
<td>/u003/app/appmgr</td>
</tr>
<tr>
<td>Oracle Apmaas Agent Type</td>
<td>premain</td>
</tr>
<tr>
<td>Oracle Apmaas Repackaged Com</td>
<td>oracle.diagnostics.instrumentor.instrumentor.ClassInfoMapMaxSize</td>
</tr>
</tbody>
</table>
But wait there's more...
Full logging is now shown on screen
How do you assess your third party?
The questions to consider to reduce potential cyber risk:

1. Do you know how third parties are accessing the platform?
2. How often is the platform assessed for potential vulnerabilities?
3. How is sensitive information (i.e., the third parties and your organization’s) being stored?
Questions?

ASK AWAY!
What is third party risk management?

Third Party Risk Management (TPRM) is an essential component of any organizational cybersecurity risk management program. ServiceNow defines TPRM as “enabling an organization to monitor and assess the risk posed by third parties to identify where it exceeds the threshold set by the business.”

The problem is that not all TPRM functions are free of risk themselves. In fact, our research indicates that some functions even introduce the very thing they are designed to suppress information useful to attackers for compromising your, or even their, organizations.