Managing the Information Security Risk of Your Data Across Your Third Parties
Q1 2018

Who is Opus?

- Opus is leading SaaS provider of Risk and Compliance solutions to the Global 2000.
- Our proven solutions address critical Know Your Customer (KYC) and Third Party Management requirements.
- Our target market is Global 2000 customers with significant regulatory demands and a dynamic network of suppliers, customers and third parties.
- Our customers include the world’s largest and best-known banks and corporations.

Our solutions help address critical Know Your Customer (KYC), Third Party and Master Data management requirements

Know Your Vendor/Know Your Third Party (Hiperos 3PM)
Know Your Customer (Alacra Compliance)
Manage Your Data
Our global customers include

- AstraZeneca
- Microsoft
- S&P Global
- Standard Chartered
- PayPal
- PricewaterhouseCoopers
- ING
- Metro Bank
- Huntington
- PNC
- Wachovia
- French Life Financial
- AG Rodolphe
- Halliburton
- BMO Capital Markets

Information security professionals today are struggling

What do you predict will happen to your career in 2018?

More than one response permitted

- My job/role will remain essentially the same: 69%
- I will take a new role within my company that will help me prevent security breaches: 41%
- I will completely change careers: 36%
- I will transition to a leadership position: 27%
- I will transition to a management position: 23%
- I will lose my job in my current position: 17%
- I will lose my job completely: 16%
- I will lose my current job of security: 0%
- Other: 3%

CISOs are feeling the stress -- even making job moves.

Risks are escalating quickly

Is your company more likely to have a data breach or cyber attack in 2018?

- No: 33%
- Yes: 67%
They can’t control the people around them

Which of the following threats do you worry most about in 2018?

- Competence of in-house staff
- Insider threats
- Malware
- Third party data breach
- Insider threats in non-technical roles
- Outsource services failure
- Inadequate budget
- Inadequate policy and procedures
- Inadequate training

Source: Ponemon Jan 2018

And one of their biggest worries is increasing third party risk

Has your concern about experiencing a data breach caused by a business partner, vendor or contractor (third party) increased, stayed the same or decreased?

- 39% increased
- 28% stayed the same
- 10% decreased
- 2% significantly decreased
- 21% increased significantly

Why are third parties such a significant vector for information security risk?

- Hackers realize large companies have hardened their infrastructures
- Hackers search for the weakest links: often third party business partners
- You may spend millions securing internal networks, but not external
- IT functions increasingly outsourced to third parties
- Can you control how your business partners and vendors defend their networks and your data?
Why is third party information security risk so tough to manage?

- 56% of businesses have experienced a third-party data breach in the last year
- Only 17% of businesses feel their third-party management processes are highly effective
- 65% feel they don’t have the resources to tackle third party risk at all

57% Do Not Have a List of Third Parties with Whom They Share Sensitive Data

- 20% Yes
- 60% No
- 20% Unsure

65% Are Not Confident a Third Party Would Notify Them of a Data Breach

- 30% Third party vendor
- 31% Nth party vendor
- 11% Unsure
- 28% Do Not Know
60% Do Not Evaluate the Security and Privacy Practices of Third Parties

Why?
1. We don’t have the internal resources to check or verify
2. The data shared with the third party is not considered sensitive/confidential
3. The third party is subject to data protection regulations that are intended to protect our information
4. The third party is subject to contractual terms
5. We rely on the business reputation of the third party
6. We have confidence in the third party’s ability to secure information
7. We have insurance that limits our liability in the event of a data breach

New regulations, new challenges

“The General Data Protection Regulation (GDPR) is the biggest change to data protection law in a generation”

Elizabeth Denham
UK Information Commissioner

So what can we do about it?
Best practices for information security
Eight Third-Party Risk Management Practices that Reduce Likelihood of Data Breach

<table>
<thead>
<tr>
<th>Practice</th>
<th>Likelihood of Breach when Governance Practice is Deployed</th>
<th>Likelihood of Breach when Governance Practice is Not Deployed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluation of the security and privacy practices of all third parties</td>
<td>40%</td>
<td>66%</td>
</tr>
<tr>
<td>Inventory of third parties with whom you share information</td>
<td>40%</td>
<td>66%</td>
</tr>
<tr>
<td>Frequent review of third-party management policies and programs</td>
<td>47%</td>
<td>63%</td>
</tr>
<tr>
<td>Formation of a third-party risk management committee</td>
<td>48%</td>
<td>63%</td>
</tr>
<tr>
<td>Visibility into third parties with whom you do not have a direct relation</td>
<td>55%</td>
<td>66%</td>
</tr>
<tr>
<td>Accountability for proper handling of third-party risk management program</td>
<td>48%</td>
<td>63%</td>
</tr>
<tr>
<td>Third-party notification when data is shared with Nth parties</td>
<td>48%</td>
<td>66%</td>
</tr>
<tr>
<td>Assurance to the board of directors</td>
<td>47%</td>
<td>65%</td>
</tr>
</tbody>
</table>

Best Practices: Reducing Third Party Breaches

- Evaluating the security and privacy practices of all third parties
  Reduces the likelihood of a breach from 66% to 46%
- Having a comprehensive list of all third parties with access to data
  Reduces the likelihood of breach from 65% to 46%
- Frequently reviewing third-party management policies and programs
  Reduces the likelihood of breach from 65% to 47%

Best practice for evaluating third party InfoSec: Control frameworks

- 84% of IT and security professionals in the US leverage a security framework
- NIST CSF, ISO 27001, CIS popular options
- 50% of organizations are anticipated to implement NIST Cyber Security Framework by 2020
A Controls Assessment Process

1. **SEGMENT & SCOPE**
   - Stratify third parties by materiality, determine level of assessment.
   - Identify data and systems touched to drive scoping of relevant controls, calculate inherent risk.

2. **ASSESS**
   - Collect due diligence questionnaires and document artifacts.
   - Perform audit: Assess vendor control effectiveness.

3. **REMEDIATE**
   - Prescribe remediation for ineffective controls.
   - Report residual risk.

4. **MONITORING**

---

Thank you

Download our reports:
www.opus.com/infosec

Contact Info:
Sam Mele
samuel.mele@opus.com
www.opus.com