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
- Fifth Third Bank
- Charles Schwab
- BB&T
- Signet Jewelers
- Arconic
- Metro Bank
- Huntington
- Webster Bank
- DocuSign
- Sherwin-Williams
- TD Bank
- BNP Paribas
- Sun Life Financial
- Credit Agricole
- AIG
- Halliburton
- ABS
- BMO
Information security professionals today are struggling

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

More than one response permitted

- My job will become more stressful: 69%
- I will make a lateral move within my company, but not into IT security: 44%
- I will completely change careers: 41%
- I will join another company, but not into IT security: 36%
- I will receive a promotion: 27%
- I will be terminated or demoted: 23%
- My salary will increase: 17%
- I will retire: 11%
- My job will become less stressful: 9%
- Other: 3%

Source: Ponemon January, 2018

Risks are escalating quickly

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

- Yes: 67%
- No: 33%

Source: Ponemon Jan 2018
They can’t control the people around them

Which of the following threats do you worry most about in 2018?
More than one response permitted

- The lack of competent in-house staff: 70%
- A data breach: 66%
- A cyber attack: 59%
- Inability to reduce employee negligence: 54%
- Ransomware: 48%
- Malicious inside threat due to unsecured IT devices in the workplace: 47%
- A third party data breach: 42%
- Inadequate budget: 34%
- Inability to reduce malicious insider risk: 25%
- A compliance failure: 25%
- A nation state attack: 19%
- None of the above: 7%
- Other: 4%

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?

- Decreased: 10%
- Significantly decreased: 2%
- Stayed the same: 28%
- Increased significantly: 21%
- Increased: 39%

Source: Ponemon January 2018
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

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

- Evaluation of the security and privacy practices of all third parties
- Inventory of all third parties with whom you share information
- Frequent review of third-party management policies and programs
- Formation of a third-party risk management committee
- Visibility into third or Nth parties with whom you do not have a direct relationship
- Accountability for proper handling of third party risk management program
- Third party notification when data is shared with Nth parties
- Assurance to the board of directors

Likelihood of a breach when the governance practice is deployed
Likelihood of a breach when the governance practice is not deployed

- 46% to 66%
- 46% to 65%
- 47% to 65%
- 48% to 63%
- 48% to 63%
- 49% to 63%
- 50% to 62%
- 51% to 61%
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 the audit: Assess vendor control effectiveness

3. REMEDIATE
   - Prescribe remediation for ineffective controls
   - Report Residual Risk

Thank you

Download our reports:
www.opus.com/infosec

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