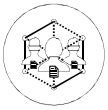
Managing the Information Security Risk of Your Data Across Your Third Parties

Q1 2018

Who is Opus?

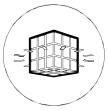
- Opus is leading SaaS provider of Risk and Compliance solutions to the Global 2000.
- Our proven solutions address critical Know Your Customer (KYC) and Third Party Management requirements.
- Our target market is Global 2000 customers with significant regulatory demands and a dynamic network of suppliers, 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

Baker Hughes · BNP Paribas · Sun Life Financial · Crédit Agricole

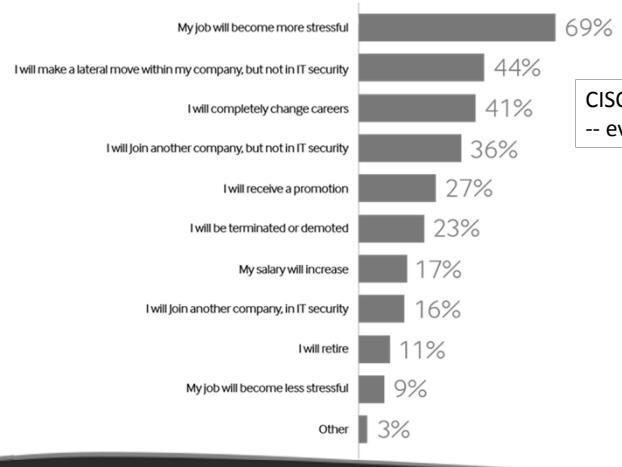
AXA · Halliburton · ABS · BMO

opus

4

Information security professionals today are struggling

What do you predict will happen to your career in 2018?
More than one response permitted



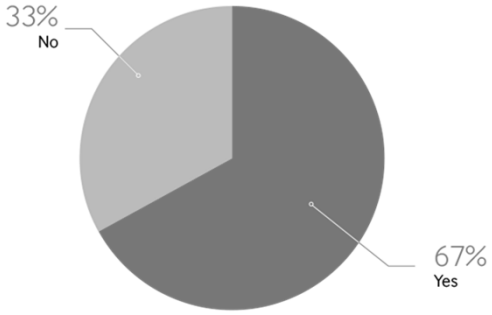
CISOs are feeling the stress -- even making job moves.

opus

Source: Ponemon January, 2018

Risks are escalating quickly

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

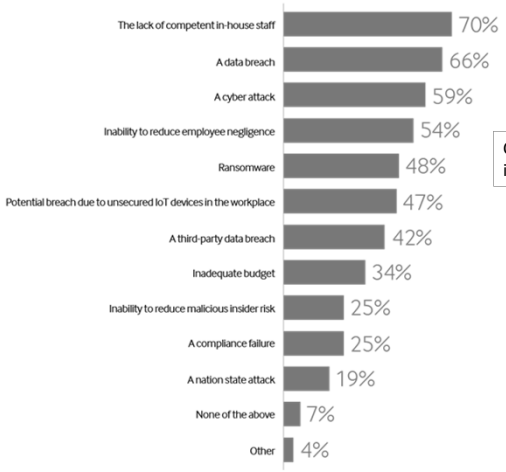


opus

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



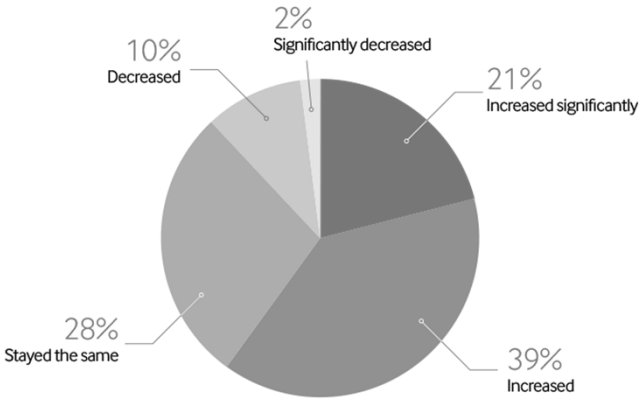
Competence of in-house staff is the number one concern…

opus

Source: Ponemon Jan 2018

And one of their biggest worries is increasing <u>third party</u> 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?



opus

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?*

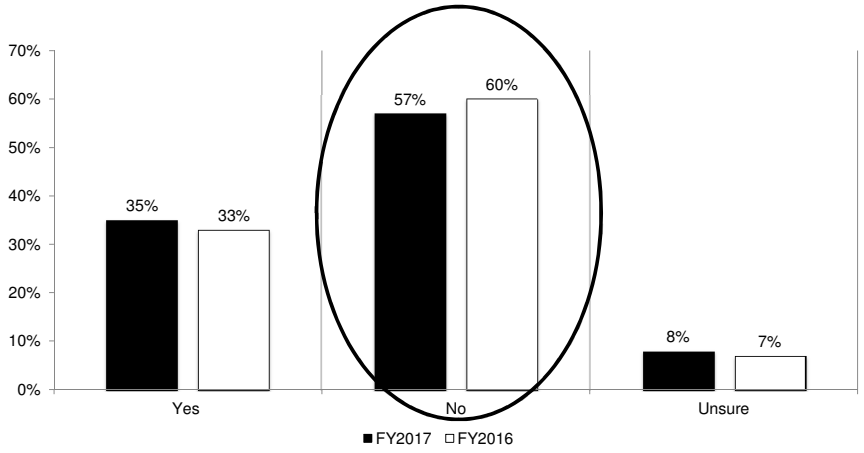
Why is third party information security risk so tough to manage?

56% of businesses have experienced a third-party data breach in the last year

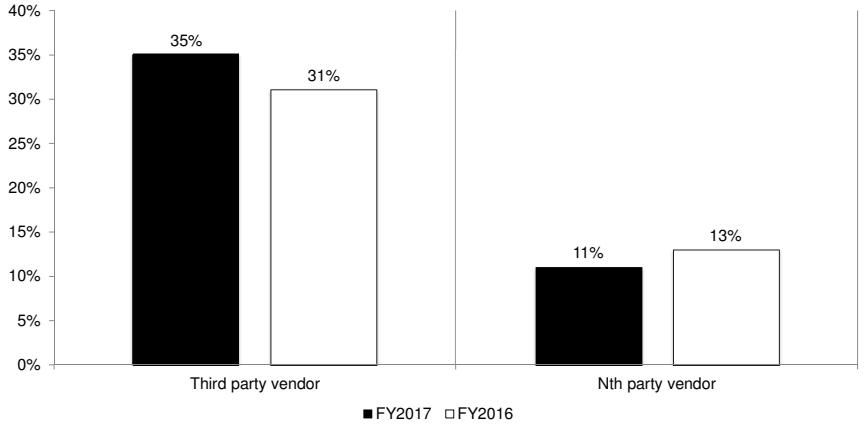
Only **17%** of businesses feel their third-party management processes are highly effective

65% feel they don't have they 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"

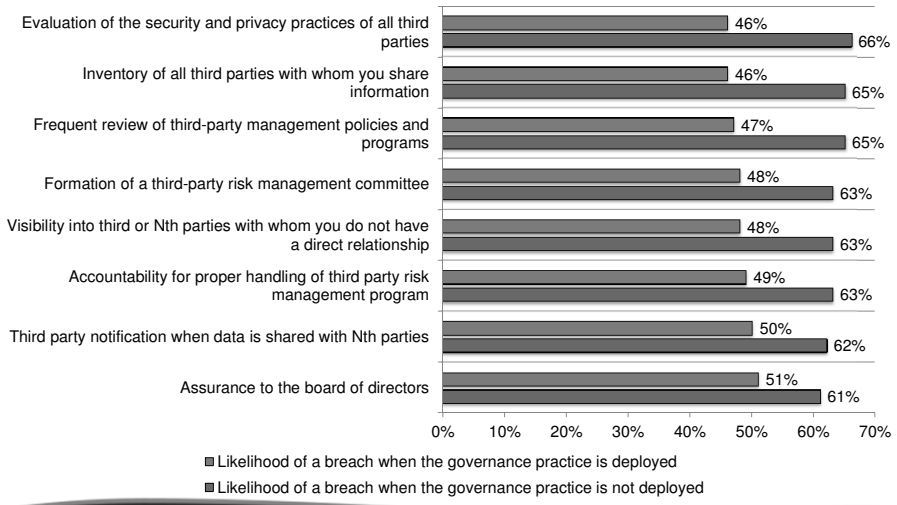
Elizabeth Denham
UK Information Commissioner

So what can we do about it?

Best practices for information security

opus
Free Your Business

Eight Third-Party Risk Management Practices that Reduce Likelihood of Data Breach



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%**

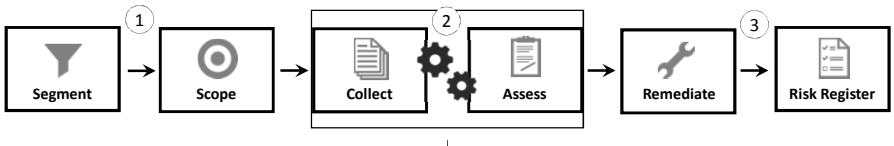
Frequently reviewing third-party management policies and programs

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



NIST CSF · SHARED ASSESSMENTS · RAPIDRATINGS · BITSIGHT · riskrecon · SecurityScorecard

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

MONITORING

Thank you

Download our reports:

www.opus.com/infosec

Contact Info:

Sam Mele
samuel.mele@opus.com
www.opus.com

opus
Free Your Business