

Protecting Your Company From Data Breaches

October 2018

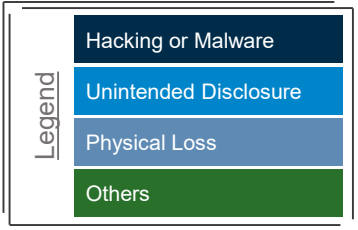
ALVAREZ & MARSAL



Third-Party Data Breach | Did You Know?

In 2017, 30% of the breaches were attributable to third-party providers. A lack of controls, integrated systems and security and streamlined reporting contributes to the challenges faced by many industries.

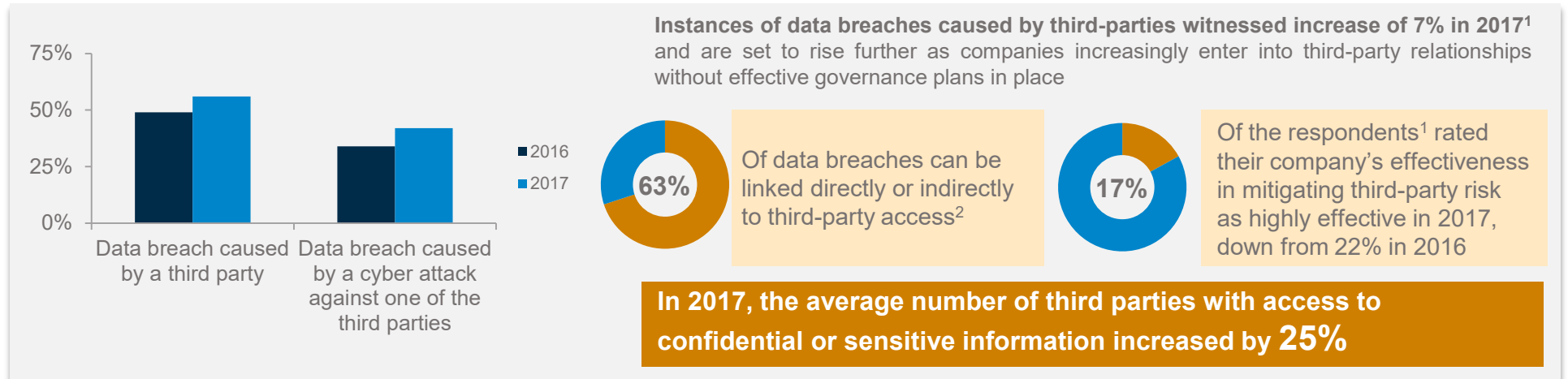
Industry	Number of Disclosed Breaches ¹	Estimated Cost (\$ million) ²	Types of Breaches (%)
Healthcare	328	1,187.4	46% Hacking or Malware, 33% Unintended Disclosure, 18% Physical Loss, 3% Others
Technology	48	173.8	75% Hacking or Malware, 25% Unintended Disclosure
Retail	40	144.8	46% Hacking or Malware, 33% Unintended Disclosure, 18% Physical Loss, 3% Others
Financial Services	40	144.8	46% Hacking or Malware, 33% Unintended Disclosure, 18% Physical Loss, 3% Others
Government	17	61.5	47% Hacking or Malware, 47% Unintended Disclosure, 6% Others
Education	16	57.9	50% Unintended Disclosure, 31% Hacking or Malware, 13% Physical Loss, 6% Others
Food	11	39.8	91% Hacking or Malware, 9% Physical Loss
Hospitality	11	39.8	100% Hacking or Malware
Home and Leisure	6	21.7	83% Hacking or Malware, 17% Unintended Disclosure
Nonprofit	6	21.7	67% Hacking or Malware, 33% Unintended Disclosure



Note: 1) Based on the data sourced from Privacy Rights Clearinghouse capturing data breaches across industries in the US for full year 2017
 2) According to a new report by Protenus, at least 30% of all breaches reported to HHS' public breach tool can be traced back to business associates and third-party vendors

Data Breach | Why Be Concerned

Despite rising third-party data breaches, more than 50% of companies surveyed either fail to maintain a comprehensive data inventory or monitor their providers security practices



Companies lack visibility into third-party relationships, but continue to share data








Note: 1) Based on a September 2017 survey conducted by Ponemon Institute on 625 respondents in the US
 2) Based on a May 2016 survey conducted by Soha Systems on >200 enterprise IT and security C-level executives, directors, and managers

Data Breach | Potential Impact

Data breaches can have a significant impact on a company's financials (fines and remediation costs) and cause loss of customers

Only **35%** of companies¹ believe that third-party providers would notify them of a breach

Target Company	Year of Breach	Affected Users	Description of the Data Breach	Impact of the Data Breach
	2014	3 billion user accounts	Hackers gained access to real names, email addresses, dates of birth, and contact numbers of users through an unknown third-party	<ul style="list-style-type: none"> Verizon (which at that time was purchasing Yahoo) slashed the purchase price by \$350 million
	2013	110 million customers	Hackers gained access and exposed personally identifiable information and payment card accounts through a third-party HVAC vendor	<ul style="list-style-type: none"> The CEO and CIO had to resign Recent company estimates indicate a loss of \$202 million
	2017	87 million	Research firm, Cambridge Analytica, purchased highly sensitive personal information of Facebook users from app developer Aleksandr Kogan (which collected user data through a psychology quiz app)	<ul style="list-style-type: none"> Immediately after the news of misuse surfaced the company lost \$75 billion in market cap Faces further regulatory actions from various authorities
	2016	57 million Uber customers and driver partners	Hackers broke into the non-encrypted data bank of a third-party provider and released names, email addresses, and mobile phone numbers of 660,000 customers and drivers	<ul style="list-style-type: none"> Paid hush money of \$100,000 to the hackers
	2017	14 million customers	NICE Systems which misconfigured a repository it had access to, exposed names, addresses, phone numbers, PINs, and account details of users	<ul style="list-style-type: none"> May face huge legal costs in event the affected customers file petitions

Note: 1) Based on a survey conducted by Ponemon Institute on 625 individuals in the US in September 2017

Data Breach | Next Steps and Considerations



1 – Create Detailed Data Map and Inventory

- Capture information of all third-party providers the company partners with and conduct due diligence on certifications and data security practices
- Map all data that is shared with third party providers
- Classify partners on the basis of risk they pose – factor in data they handle and the likelihood of a breach targeting them



2 – Include Data Security Obligations in Contracts

- Contracts with a third-party provider should include a data management framework:
 - Strategies to be implemented before data breach occurs (e.g. who has access to the data, need for insurance coverage, data security protocols)
 - Protocols on reporting data breaches and assignment of responsibility and obligations



3 – Control Access to Data

- Make use of single sign-on solutions to limit data access, which will also help limit access to authorized users



4 – Document and Evaluate Data Security Practices

- Seek expert guidance in conducting periodic evaluation of data security practices followed by the third-party providers and determine if they are meeting all requirements listed in the contract



5 – Develop Framework to Protect Yourself from Cyber Attacks

- In addition to having a sound data security framework in place, companies should also look to have cyber security insurance including third-party coverage
- Other measures include encryption of data and having a kill switch to cut-off access to data (in case of a breach)

Best in Class Evaluation Tool | Competitive Advantage

A&M's cybersecurity evaluation identifies and aggregates cyber risk across the enterprise, giving companies a deeper understanding of their overall cyber risk and potential adverse cybersecurity exposure. Our exclusive QUERI Risk Intelligence Tool provides customized and highly-focused insight into the company's preparedness for and defensive posture against a breach.

QUERI: Quantified Enterprise Risk Intelligence



QUERI ASSISTS EXECUTIVES IN UNDERSTANDING THEIR RISK

Initial intelligence gathering to inform deeper evaluation

- Unified approach to understand risk
- Identifies best practices from one portfolio to be applied to others
- Examines Data Privacy controls

Discover vulnerability causation

- Validate SME and employee understanding of compliance expectations
- Identify root causes of failure to achieve compliance maturity

Measure cybersecurity risk posture and process maturity

- Discover processes or functions not meeting management expectations
- Identify weak or absent detective and protective activities
- Establish baseline and collect historical gap closure success rates for security program



VALUE ADDED RESULTS

- Understand** your cybersecurity risks posture or maturity.
- Be informed** of the remediation costs of unacceptable cybersecurity risks.
- Discover** third party risks that negatively impact your data.
- Mitigate** risks to the company by proactively identifying and remediating risk.
- Reduce** operational and reputation risk of breaches and costs associated with a lack of preparation to manage breaches.

Experts to Call

Technology



David Bergen
Managing Director, San Francisco
+1 (415) 490 2320
dbergen@alvarezandmarsal.com



Dhiren Rawal
Managing Director, New York
+1 (212) 763 9770
[drawal@alvarezandmarsal.com](mailto:dawal@alvarezandmarsal.com)

Third Party Risk Management



Brian Smith
Managing Director, New York
+1 (212) 328 8501
brian.smith@alvarezandmarsal.com



Cyndi Joiner
Managing Director, Atlanta
+1 (404) 260 4118
cjoiner@alvarezandmarsal.com



Art Hall
Senior Director, Atlanta
+1 (404) 260 4152
ahall@alvarezandmarsal.com

Disputes & Investigation



Douglas Anderson
Managing Director, Atlanta
+1 (321) 432 8656
danderson@alvarezandmarsal.com



Art Ehuan
Managing Director, Washington DC
+1 (571) 331 7763
aeahuan@alvarezandmarsal.com



John deCraen
Senior Director, Dallas
+1 (817) 881 8879
jdecraen@alvarezandmarsal.com



Shawn Fleury
Director, San Antonio
+1 (210) 510 8578
sfleury@alvarezandmarsal.com



Billy Evans
Director, San Antonio
+1 (210) 426 8954
bevans@alvarezandmarsal.com



Adriel Ginsburg
Director, Atlanta
+1 (678) 246 9055
aginsburg@alvarezandmarsal.com