



# **Staying One Step Ahead Of Uncertainty Third Party Risk Management (TPRM)**

Sean O'Brien, Director

# Defining Third Party

Third Party Risk Management is a process for identifying and managing risks created when hiring a third party to provide goods and/or services.

Its primary focus is usually on data protection/privacy and IT security controls, but its scope depends entirely on the nature of the services provided by the third party.

Therefore, it may include operational issues such as business continuity and disaster recovery, financial integrity, regulatory compliance, and the suppliers own third party risk management practices.

# Emerging Supplier Risks

Increasing need for third party oversight

- Relationship between organisations and their third party suppliers has become more complicated as those third parties are increasingly being viewed as business partners
- The risks associated with working with third party suppliers have become more complicated as those third parties have emerged as more popular targets for cyber attacks.
- The regulatory environment has become more complex
- Suppliers are increasingly targeted by criminals

# 3rd Party Risk Management Is A Hot Topic



- 3rd party risk is considered serious and increasing. <sup>1</sup>
- Somewhere between 60-80% of data breaches over the past two years occur through a third party. <sup>2</sup>
- The increase in cloud and IoT are seen as the primary contributing factors to the increase in 3rd party risk. <sup>3</sup>
- Despite the seriousness of third party risk, it is not a primary risk management objective. <sup>3</sup>
- The consequences of not managing third party risk can be costly. <sup>4</sup>
- Lack of formal programs affects the ability to mitigate third party risk. <sup>3</sup>

1. Ponemon Institute , Supplier Risk Management Survey, May 2016

2. PWC, 2016

3. Tone at the Top and Third Party Risk Report , Ponemon Institute, May 2016

4. Mandiant M-Trends Report 2016

# You're Only As Strong As Your Weakest Link

DEBENHAMS  
FLOWERS

eCommerce provider  
hacked, 2017

- 26,000 website customer accounts exposed
- Third-Party service provider targeted to gain access to customer payment details
- Attackers had access to the Third-Party's internal systems for more than six weeks

 **TARGET**

\$18.5m fine for breach of  
Customer transaction data

- HVAC service provider software used as a back door to access Target's payment system network
- Malware uploaded to tills exposing approx. 41m Customer credit/debit card accounts over 3 weeks in 2013
- Fined \$18.5m by US authorities in May 2017.  
Total cost of breach and remediation calculated at \$202m.

TalkTalk

Total fines of £500,000  
from the ICO

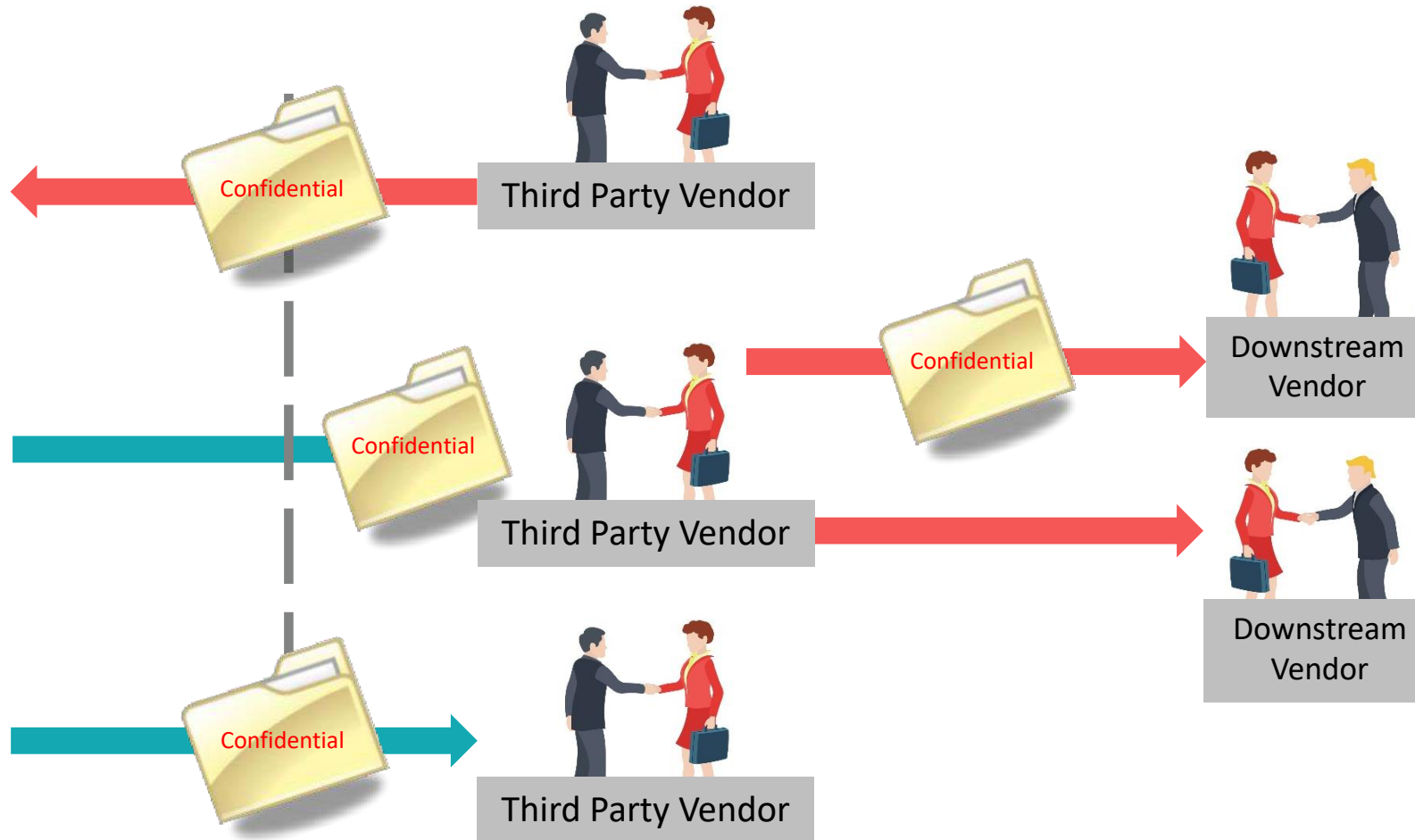
- 21,000 Customers compromised in 2014 by "unauthorised and unlawful access" by staff at call centre in India
- Data gained used in phone scam to build Customer trust to then release account and financial details
- Fined £100k in August 2017 after £400k fine for hack in 2015

 **UniCredit**

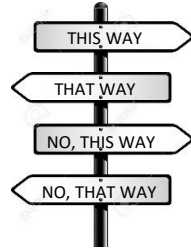
2016 Breach not  
identified until 2017

- Around 400,000 Italian bank accounts accessed in one of Europe's largest data breaches
- Unauthorized access through Italian third party provider to Italian customer data was the cause of the breach
- Breaches occurred in September and October 2016 but only uncovered in July 2017

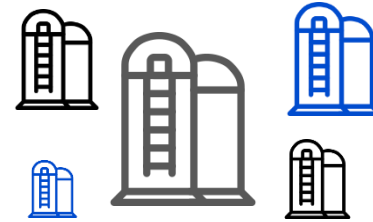
# Data Supply Chain



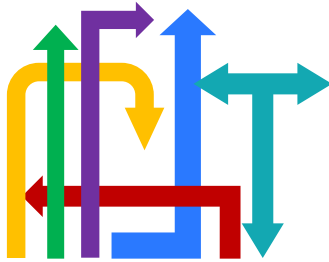
# Vendor Risk Management Problem



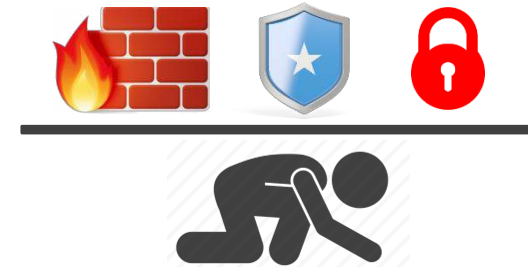
Rapidly Changing Landscape



Not Policy or Process Driven



Inconsistent Process & Framework



Supplier Bypasses IT Security



Lack of Enforcement or Ownership

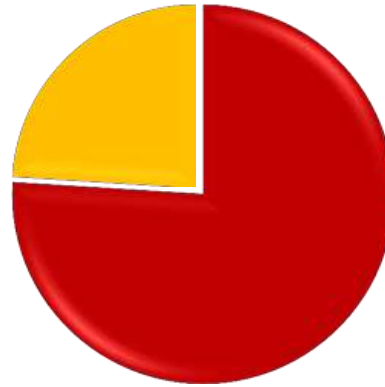


# Interesting Statistics

**Only 24%**

of respondents require third- party suppliers or partners to comply with baseline security procedures

– PWC Third Party Risk Management April 2015



**76% of data breaches**

analysed by TrustWave resulted from a third-party which introduced the security deficiencies that were ultimately exploited.

– Trustwave 2016 Global Security Report



**less than 1 in 5** enterprises are conducting security assessments from 3<sup>rd</sup> parties — Veracode 2012 State of Software Security Report

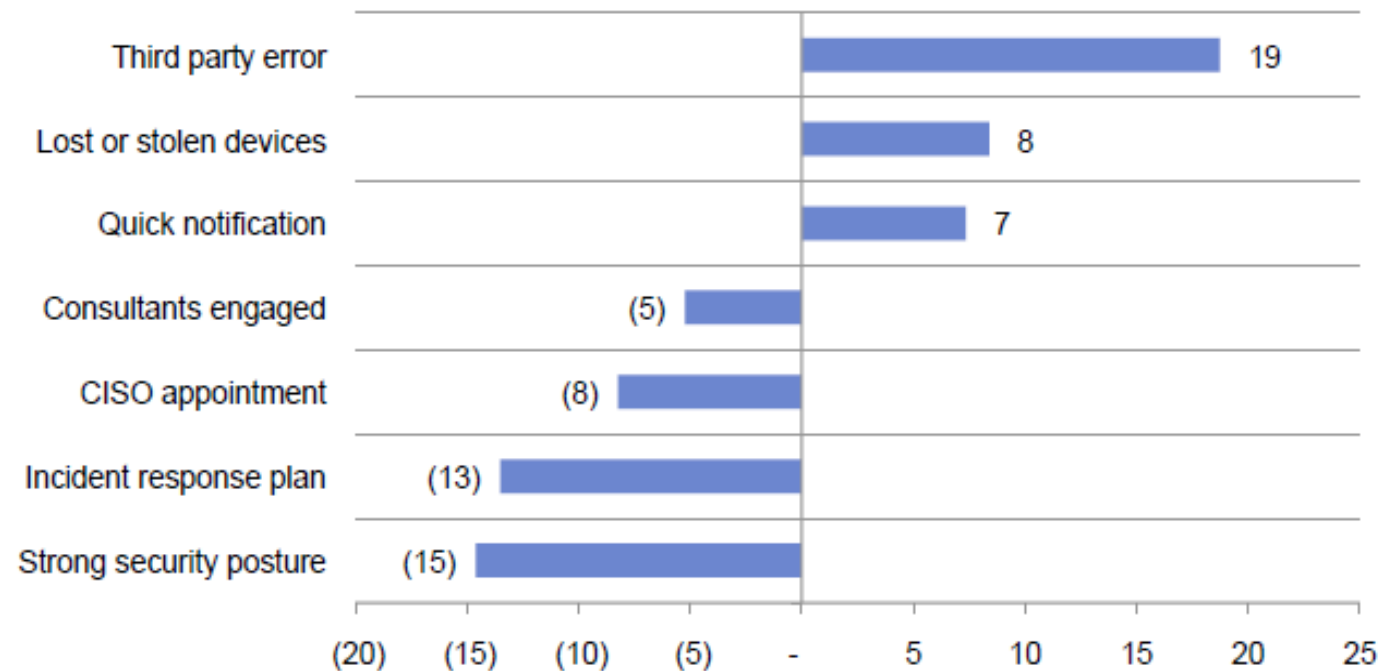


# 3<sup>rd</sup> Party Error & Data Loss Cost

As shown in Figure 9, a strong security posture, incident response planning CISO appointments and consulting support decreases the per capita cost of data breach (shown as negative numbers).

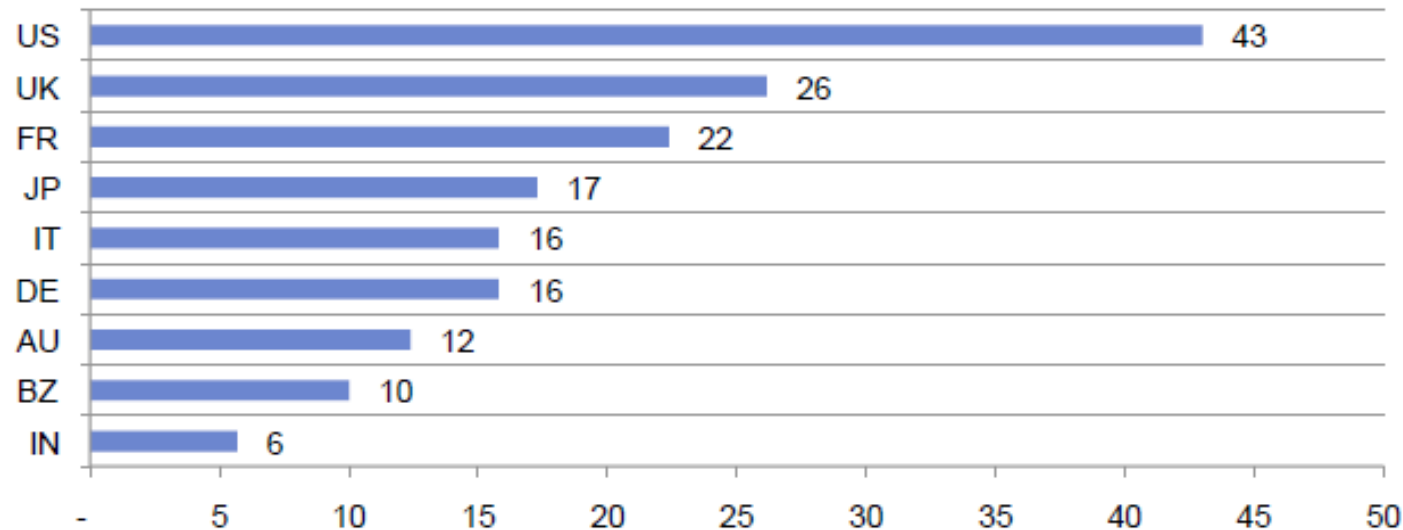
Third party errors, lost or stolen devices and quick notifications increase the per capita cost of data breach (shown in positive numbers).

**Figure 9. Impact of seven factors on the per capita cost of data breach** Consolidated view (n=277). Measured in US\$



Source: 2016 Cost Data Breach Study; Ponemon Institute; May 2016

# 3<sup>rd</sup> Party Error & Data Loss Cost



Source: 2016 Cost Data Breach Study; Ponemon Institute; May 2016

Figure 11 shows the factors that increased the cost of data breach.

On average, third party errors increased the cost of data breach by as much as \$43 per record in the US.

In the case of Brazil and India, such incidents increased the cost by only \$10 and \$6, respectively.

**Figure 11. Third Party Error (US\$)**

# Where Do The Risks Lie?

- ! Companies are spending millions of pounds on securing their own environments, when malicious insider and hack attacks represent less than 5% of data loss incidents in the past two years
- ! Less than 30% of UK companies have a formal Supplier Risk Management program
- ! Of those 30%, less than 10% have a standardised formal process

# Where to Start?

- Know your third parties
  - Third party identification – who are they and what do they do?
    - Who are your third party service providers?
    - What services do they provide?
    - What data/systems do they have access to?
- Most companies do not maintain a current comprehensive list of their suppliers!

# Supplier Risk Management Framework – What does it look like?

## Program Definition

*How to secure your program*

- ✓ Governance Models
- ✓ Policies, Standards & Procedures
- ✓ Contracts & Agreements

## Program Execution

*How to run your program*

- ✓ Risk identification & Analysis
- ✓ Personnel, Skills, & Expertise
- ✓ Communication & Information Sharing

## Program Management

*How to monitor & adapt your program*

- ✓ Tools, Measurements & Analysis
- ✓ Monitoring & Review

# Supplier Risk Management Framework – Where to start?

- Establish a formal governance model or organisational structure to manage third party risk
- Establish clearly defined strategies, goals and objectives for your supplier risk management program
- Develop a comprehensive set of policies, standards and procedures, as a foundation of your third party management program
- Define your organisations risk appetite
- Develop a risk based supplier rating model

# Problem Areas

- How to create and maintain valid and pertinent questionnaire sets?
- Excel or paper-based questionnaires
- Procurement
- Contract Management
- GDPR – Can't have a presentation without mentioning it.....
  - *(What do the ICO say about TPRM?)*



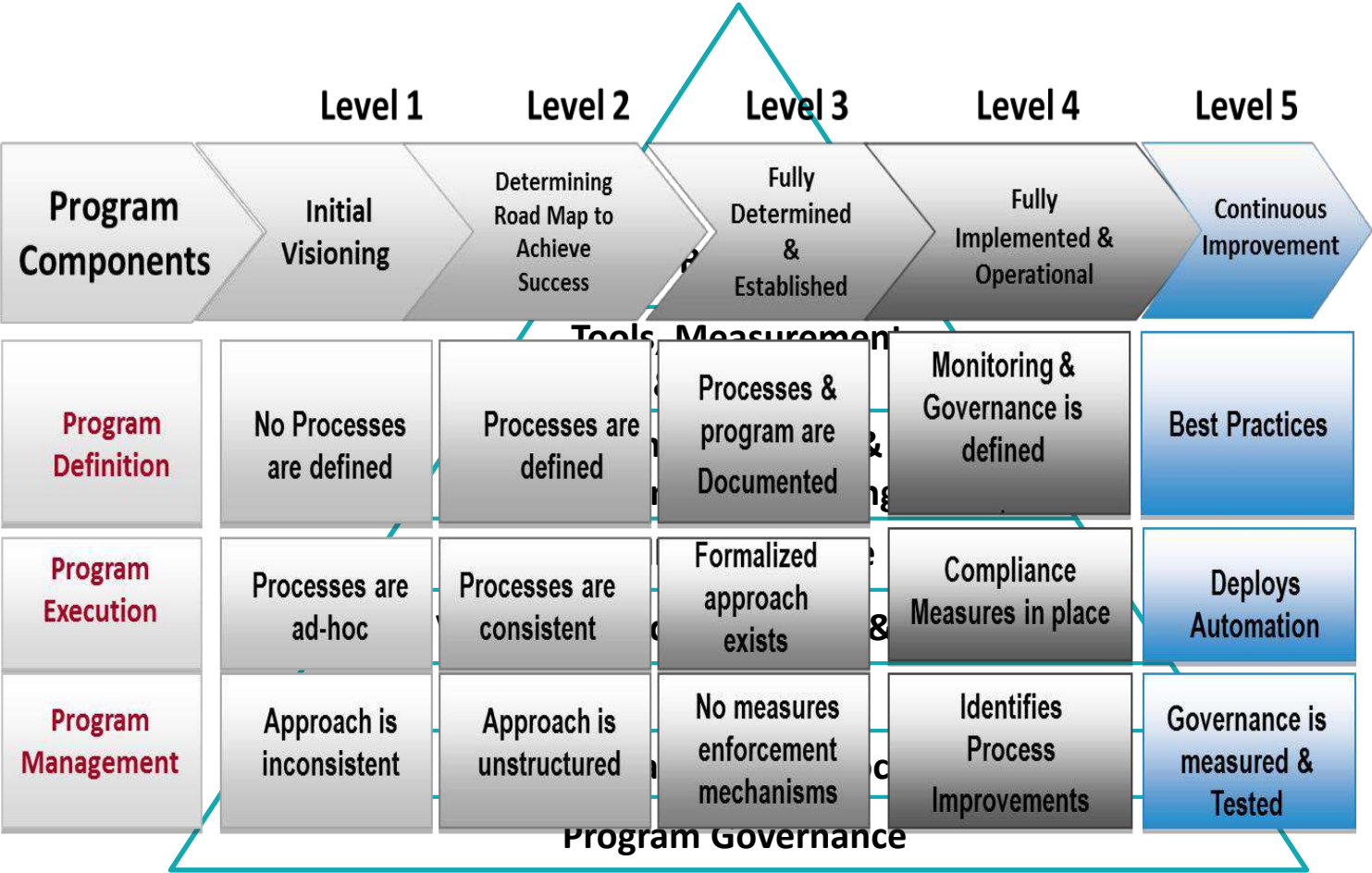
# So what does best practice look like?

- ✓ Risk-based Standardised Approach
- ✓ Risk-tiered Questionnaires
- ✓ Remote and Onsite Assessment
- ✓ Remediation Tracking
- ✓ Continuous Monitoring

# Supplier Risk Management Maturity Model (VRMMM)



# Supplier Risk Management Maturity Model (SRMMM)



# The Solution

- ✓ Standardised Formal Process
- ✓ Automate to be able to Scale
- ✓ Outsource to the Experts
- ✓ Continuously Monitor Critical Suppliers

# Introducing SupplierAssess

Taking the Pain Out of Supplier Risk Management



- A 3<sup>rd</sup> Party Supplier Assessment Service
- Experienced and qualified team of certified professional assessors (ISO 27001 Lead Auditors)
- Supplier Risk Manager Service provides automation, workflow, and a central repository for all assessment information
- Supplier Threat Monitor Service provides real-time 3<sup>rd</sup> party risk monitoring
- Commitment to providing “information anywhere, security everywhere” through established processes and service delivery methodologies

# So What Does It Do?

TPRM delivered to your desk



## Remote & On Site Assessment

- Ranks suppliers, collects evidence for the review workflow, and performs risk assessments on each Third Party supplier

## Reporting & Recommendations

- Supplier Assessment dashboard and detailed supplier assessment reports that include findings and mitigation recommendations

## Continuous Threat Monitoring

- Ongoing tracking of risk factors between assessments including Data, Operational, Financial, Brand, Regulatory events and other Geographical issues

# What Is The Process?






- › Understand organisations risk appetite and security objectives and configure Supplier Risk Manager to reflect company requirements
- › Accumulate supplier assessments and corresponding required artifacts on your behalf
- › Provide a risk recommendations report based on information accumulated, industry intelligence and contextual risk environment
- › Work with you and your suppliers to initiate risk workflow for identified gaps
- › Monitor 24/7 supplier threat intelligence with Supplier Threat Monitor



# What Are The Benefits?



-  Understand potential data loss from your suppliers within the context of their business and your business relationship
-  Automate to scale your with standardised content and a standardised process
-  Reduce the cost associated with your existing manual process and internal infrastructure

# Who We Are

Founded in 1999 | Headquartered in Cheshire, UK



- Experts in Third Party Risk and IT Security
- Shared Assessments member – only UK-based Assessment Firm
- Prevalent EMEA Channel Partner – only EMEA-based Partner
- Certified Third Party Risk Professional accredited Risk Assessors
- Clients across legal, banking, insurance, retail, and public sectors
- SupplierAssess™ managed service - unique TPRM-as-a-service offering outsourced risk assessment and analysis

# Questions?

**Sean M. O'Brien**  
Director

DDI: +44 (0) 161 476 8702  
M: +44 (0) 7973 295 997  
E: [sobrien@dvvs.co.uk](mailto:sobrien@dvvs.co.uk)



DVV Solutions Limited  
Grosvenor House, St. Thomas's Place  
Stockport, Cheshire, SK1 3TZ  
United Kingdom

[www.dvvs.co.uk](http://www.dvvs.co.uk)



Follow us at [LinkedIn.com/company/dvv-solutions](https://www.linkedin.com/company/dvv-solutions)

